Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: "Захист операційної системи Windows від brute-force атак"

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Ворона Максим Сергійович
підпис (прізвище та ініціали)

Керівник Лечаченко Т. А.
підпис (прізвище та ініціали)

Нормоконтроль Лобур Т.Б.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Вороні Максиму Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Захист операційної системи Windows від brute-force атак

Керівник роботи Лечаченко Тарас Анатолійович, PhD доктор філософії., асистент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 03 » 04 2023 року № 4/7-349

2. Термін подання студентом завершеної роботи 14.06.2023

3. Вихідні дані до роботи Вимоги до операційної системи Windows

4. Зміст роботи (перелік питань, які потрібно розробити)
Проаналізувати brute-force атаки та їх наслідки.
Проаналізувати захист від brute-force атак в операційній системі windows server 2022
Розробити та протестувати тестування систему автоматичного блокування ip-адрес зловмисників
Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Тема, мета, задачі. Поняття brute-force атаки. Методи захисту від brute-force атак. Захист від brute-force атак в операційній системі windows server 2022. Захист від brute-force атак з зовнішньої мережі. Схема підключення корпоративної мережі до мережі Інтернет. Приклад налаштування правил брандмауера на обладнанні Mikrotik. Захист від атак з локальної мережі. Налаштування політики паролів в операційній системі Windows Server 2022. Здійснення brute force атаки на RDP –сервер. Brute-force атака на RDP-сервер за допомогою Hydra. Результати проведення brute-force атаки на RDP-сервер. Повторна brute-

force атака із використанням політики паролів та облікових записів. Розробка та тестування системи автоматичного блокування ip-адрес зловмисників. Написання сценарію PowerShell. Автоматизація процесу блокування IP. Тестування системи автоматичного блокування IP зловмисника. Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Пилипець М.І., проф. кафедри МТ		

7. Дата видачі завдання 20.01.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.01 – 23.01	Виконано
2.	Підбір джерел для аналізу brute-force атаки та їх наслідки	25.01 – 05.02	Виконано
3.	Опрацювання джерел в галузі дослідження	06.02 – 20.02	Виконано
4.	Провести аналіз методів захисту від brute-force атаки	22.02 – 12.03	Виконано
5.	Здійснення brute-force атаки на RDP -сервер	15.03-25.03	Виконано
6.	Налаштування системи автоматичного блокування IP зловмисника	25.02 – 10.04	Виконано
7.	Оформлення розділу «Brute-force атаки та їх наслідки»	10.02 – 05.03	Виконано
8.	Оформлення розділу «Захист від brute-force атак в операційній системі windows server 2022»	26.03 – 04.05	Виконано
9.	Оформлення розділу «Розробка та тестування системи автоматичного блокування ip-адрес зловмисників»	12.04-20.04	
10.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	25.04 – 10.05	Виконано
11.	Оформлення кваліфікаційної роботи	23.05 – 08.06	Виконано
12.	Нормоконтроль	10.06 – 15.06	Виконано
13.	Перевірка на плагіат	20.06 – 22.06	Виконано
14.	Попередній захист кваліфікаційної роботи	14.06 – 15.06	Виконано
15.	Захист кваліфікаційної роботи	22.06.2023	

Студент _____ Ворона М.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Лечаченко Т. А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Захист операційної системи Windows від brute-force атак // Кваліфікаційна робота ОР «Бакалавр» // Ворона Максим Сергійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-41 // Тернопіль, 2023 // С. 58 , рис. – 22, табл. – - , кресл. – 20 , додат. – -.

КЛЮЧОВІ СЛОВА: WINDOWS, RDP, FIREWALL, POWERSHELL, РОУТУР, BRUTE-FORCE, NAT.

Кваліфікаційна робота присвячена дослідженню та захисту від brute-force атак на операційну систему Windows Server 2022. Атаки такого типу становлять серйозну загрозу для безпеки інформаційних систем, порушуючи конфіденційність та доступ до даних. У роботі розглянуті різні механізми та заходи безпеки для ефективного захисту. Аналізуються механізми політики паролів, блокування паролів після невдалих спроб та фільтрації трафіку через брандмауер. Для виявлення та блокування атак була розроблена система на базі PowerShell, яка аналізує журнал подій та автоматично блокує IP-адреси зловмисників через Windows Firewall. Моніторинг забезпечується планувальником завдань, що виконує сценарії при заданих умовах.

Розроблена система є універсальною та може бути застосована для виявлення та блокування brute-force атак на Windows Server. Результати роботи дозволять підвищити рівень безпеки операційної системи та забезпечити надійність інформаційних ресурсів. Розроблені методи можуть бути використані адміністраторами систем для покращення захисту серверів.

Кваліфікаційна робота також може бути використана в навчанні. Розроблені методи та сценарії є прикладами та практичними вправами для студентів, які вивчають безпеку операційних систем. Вона дозволяє ознайомитися з концепцією brute-force атак та навчитися захищати системи від таких загроз.

ABSTRACT

Windows operating system protection against brute-force attacks // Thesis of educational level "Bachelor"// Vorona Maksym Serhiiovych // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБс-41 // Ternopil, 2023 // P. 58 fig. - 22, tab. - _-_, chair. - 20 , added. – -.

Keywords: WINDOWS, RDP, FIREWALL, POWERSHELL, РОУТУР, BRUTE-FORCE, NAT.

The qualification work is devoted to the study and protection against brute-force attacks on the Windows Server 2022 operating system. Attacks of this type pose a serious threat to the security of information systems, violating confidentiality and access to data. The paper discusses various mechanisms and precautions for effective protection. The mechanisms of password policy, blocking passwords after unsuccessful attempts and filtering traffic through the firewall are analyzed. To detect and block attacks, a PowerShell-based system was developed that analyzes the event log and automatically blocks the IP addresses of intruders through Windows Firewall. Monitoring is provided by the task scheduler, which executes scripts under specified conditions.

The developed system is universal and applicable for detecting and blocking brute-force attacks on Windows Server. The results of the work will improve the security level of the operating system and ensure the reliability of information resources. The developed methods can be used by system administrators to improve server security.

Qualifying work can also be used in training. The developed methods and scenarios are examples and practical exercises for students who study the security of operating systems. It allows you to familiarize yourself with the concept of brute-force attacks and learn how to protect systems from such threats.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

RDP	—	Remote Desktop Protocol
IDS	—	Intrusion Detection System
IPS	—	Intrusion Prevention System
DoS	—	Denial of Service
NAT	—	Network Address Translation
VPN	—	Virtual Private Network
SMB	—	Server Message Block
FTP	—	File Transfer Protocol

ВСТУП

Сучасні інформаційні системи залежать від безперервного та надійного доступу до даних та ресурсів. Операційна система Windows Server 2022 виступає важливим елементом інфраструктури багатьох організацій, забезпечуючи цілісність, конфіденційність та доступність їх даних. Однак brute-force атаки, можуть становити значну загрозу для безпеки операційної системи.

Brute-force атаки представляють собою один з найпоширеніших методів зламу систем, заснований на систематичних спробах перебору можливих комбінацій паролю та логіну. Успішне виконання такої атаки може призвести до несанкціонованого доступу до системи, втрати конфіденційних даних, порушення приватності користувачів та завдання серйозних фінансових збитків.

Ця кваліфікаційна робота має на меті дослідити поняття brute-force атак, їх наслідки та можливі методи захисту операційної системи Windows Server 2022 від таких атак. Основний акцент буде зосереджено на захисті від brute-force атак та механізмах, що доступні у Windows Server 2022.

Додатково, буде розглянута схема підключення корпоративної мережі до Інтернету через роутер з брандмауером, яка дозволяє забезпечити фільтрацію трафіку та запобігти несанкціонованому доступу до сервера з зовнішньої мережі. Також будуть досліджені вбудовані механізми захисту, такі як політика паролів та блокування пароля після кількох невдалих спроб входу через RDP для захисту від brute-force атак з локальної мережі і не тільки.

З метою ефективного виявлення та блокування brute-force атак, буде розроблений сценарій PowerShell для аналізу журналу подій на Windows Server, зокрема, події 4625, яка пов'язана з невдалими спробами входу. При виявленні атаки, буде реалізовано автоматичне блокування IP-адреси зловмисника за допомогою Windows Firewall.

Для постійного моніторингу наявності атаки brute-force, буде використано планувальник завдань, який спрацьовуватиме при заданих умовах, виконуючи сценарій PowerShell для блокування IP зловмисника.

Результати цієї дипломної роботи сприятимуть підвищенню рівня захищеності операційної системи Windows Server 2022 від brute-force атак, допомагаючи забезпечити безпеку та надійність інформаційної інфраструктури організацій.

1 BRUTE-FORCE АТАКИ ТА ЇХ НАСЛІДКИ

1.1 Поняття brute-force атаки

Brute-force атака (або атака "грубої сили") є методом зламу системи шляхом систематичної перебору всіх можливих комбінацій паролів та логінів для отримання правильного пароля та логіна.

Механізм brute-force атаки базується на послідовній спробі використання всіх можливих комбінацій паролів та логінів для входу до цільової системи. Зловмисник використовує автоматизовані засоби або програми, які пробують різні комбінації символів (літер, цифр, символів пунктуації) до тих пір, поки не буде знайдено правильний пароль та логін [1].

Цей метод може зайняти тривалий час, особливо якщо пароль або ключ є достатньої довжини та складності. Зловмисник може використовувати різні варіації алгоритмів та стратегій для прискорення процесу, такі як використання словникових атак.

Після успішного виконання brute-force атаки зловмисник отримує несанкціонований доступ до системи, що може мати серйозні наслідки, включаючи доступ до конфіденційної інформації, порушення приватності користувачів, втрату даних або виконання зловмисних дій в рамках цільової системи.

Застосування відповідних методів та заходів захисту є необхідним для запобігання brute-force атакам та забезпечення безпеки операційних систем та інформаційних систем загалом.

Brute-force атаки застосовуються з різноманітними цілями. Основні з них включають:

- Перехоплення облікових записів. Зловмисники можуть використовувати brute-force атаки для злому паролів користувачів з метою отримання несанкціонованого доступу до їх облікових записів. Це може дати зловмиснику повний контроль над системою та даними користувача;

- Злам веб-сайтів. Зловмисники можуть спробувати зламати паролі адміністраторів веб-сайтів, щоб отримати доступ до панелі управління та змінити вміст сайту або виконати інші злочинні дії;
- Розшифрування шифрованих даних. Якщо дані зашифровані за допомогою сильного шифру, зловмисники можуть використовувати brute-force атаки, спробуючи всі можливі комбінації ключів, для розшифрування цих даних;
- Злам паролів Wi-Fi. За допомогою brute-force атак, зловмисники можуть спробувати зламати паролі Wi-Fi мереж, щоб отримати несанкціонований доступ до Інтернету або виконати інші атаки в рамках бездротової мережі;
- Тестування системи на стійкість до атак. Етичні хакери та безпекові аналітики можуть використовувати brute-force атаки для тестування системи на стійкість до таких атак. Це дозволяє виявити слабкі місця та вразливості системи та вжити заходів для їх усунення.

Для виконання brute-force атаки можуть бути використані різні способи та інструменти. Зловмисники можуть використовувати програми або скрипти, що автоматизують процес генерації та перевірки паролів. Крім того, вони можуть використовувати словники, списки популярних паролів або власноруч створені комбінації символів.

Успішність brute-force атаки залежить від довжини та складності пароля, обчислювальних можливостей зловмисника та заходів захисту, які використовуються на цільовій системі. Чим складніший пароль та чим більші ресурси потрібні для виконання атаки, тим менша ймовірність успіху brute-force атаки.

Додатково до механізму brute-force атаки, існують певні методи та техніки, які зловмисники можуть використовувати для підвищення ефективності атаки. Ось кілька з них:

- Словники та варіації. Замість перебору всіх можливих комбінацій символів, зловмисники можуть використовувати словники, які містять часто вживані паролі або поширені слова. Вони також можуть

застосовувати різні варіації, такі як додавання чисел або символів до словних паролів;

- Атаки з використанням ресурсів. Зловмисники можуть використовувати розподілені системи або ботнети для розпаралелювання brute-force атак. Це дозволяє їм використовувати більшу кількість обчислювальних ресурсів і прискорити процес перебору паролів;
- Атаки з використанням контексту. Замість загального перебору паролів, зловмисники можуть використовувати специфічний контекст атаки. Наприклад, вони можуть використовувати інформацію про користувачів, таку як імена, дати народження або інші персональні дані, для `використання в паролях для підбору.
- Оптимізація порядку спроб. Замість послідовного перебору всіх комбінацій, зловмисники можуть використовувати евристики та оптимізувати порядок спроб відповідно до ймовірності успіху. Наприклад, вони можуть спочатку спробувати більш ймовірні комбінації перед переходом до менш ймовірних.

Розуміння цих методів та технік може допомогти у розробці ефективних заходів захисту від brute-force атак та підвищенні безпеки операційних систем та інформаційних ресурсів.

1.2 Мета та наслідки brute-force атак

Мета використання brute-force атак полягає в незаконному отриманні доступу до об'єктів, ресурсів або інформації, на яку зловмисник не має легальних прав доступу [1]. Зловмисники можуть мати різноманітні мотиви для проведення таких атак, а саме:

- Незаконне отримання конфіденційної інформації. Успішна brute-force атака може дати зловмисникам доступ до конфіденційних даних, таких як фінансові відомості, особисті дані користувачів, комерційна та

інтелектуальна власность. Ці дані можуть бути використані для шахрайства, вимагань, шпигунства або інших негативних цілей.

- Незаконне керування системою або ресурсами. Зловмисники можуть використовувати brute-force атаку, щоб отримати незаконний доступ до системи або ресурсів із метою їх контролю та маніпуляцій. Наприклад, вони можуть зламати адміністративні облікові записи, сервери, мережеві пристрої або веб-сайти з метою виконання дій, які можуть завдати шкоди або викликати порушення безпеки.
- Незаконне використання обчислювальних ресурсів. Зловмисники можуть використовувати brute-force атаку, щоб отримати доступ до потужних обчислювальних ресурсів, таких як сервери або комп'ютери, для виконання інших кримінальних дій. Наприклад, це може бути використано для злому криптовалютних гаманців, генерації спаму, створення ботнетів, добування криптовалюти або проведення атак на інші системи.

Наслідки успішного виконання brute-force атак можуть бути серйозними і мають потенційний вплив як на індивідуальних користувачів, так і на організації. Ось деякі можливі наслідки:

- Крадіжка або витік конфіденційної інформації. Зловмисники можуть отримати доступ до конфіденційних даних, таких як фінансові відомості, особисті дані, комерційна інформація або інтелектуальна власність. Це може призвести до крадіжки ідентичності, шахрайства, порушення законодавства про захист даних, репутаційної шкоди та втрати довіри.
- Втрата контролю над системою або ресурсами. Успішна атака може дати зловмисникам невповноважений доступ до системи, мережі або ресурсів. Вони можуть виконувати дії, які призвести до втрати даних, зупинки роботи системи, поширення шкідливого програмного забезпечення або використовувати ресурси для інших злочинних цілей.
- Вплив на довіру та репутацію. Успішна brute-force атака може негативно вплинути на репутацію і довіру до організації або системи, особливо якщо це стосується недостатньо захищених облікових записів

користувачів або конфіденційних даних. Втрата даних або порушення безпеки можуть призвести до втрати клієнтів, судових позовів, втрати бізнесу та інших негативних наслідків.

Забезпечення ефективного захисту від brute-force атак є надзвичайно важливим для запобігання цим потенційним наслідкам і збереження безпеки інформаційних систем.

1.3 Загальні методи захисту від brute-force атак

Захист від brute-force атак є важливою складовою безпеки системи. Ось декілька загальних методів захисту, які можна застосовувати для запобігання успішним brute-force атакам [2]:

- Складні паролі. Використовуйте складні паролі, які складаються з комбінації великих і малих літер, цифр та спеціальних символів. Використання довгих і унікальних паролів ускладнює завершення brute-force атаки шляхом перебору всіх можливих комбінацій.
- Багаторівнева аутентифікація. Використовуйте методи аутентифікації, які вимагають не лише пароль, але й додаткові фактори, такі як одноразові паролі, біометричні дані або апаратні ключі. Це робить завершення brute-force атаки набагато складнішим, оскільки зловмиснику потрібно мати доступ до додаткових факторів аутентифікації.
- Блокування облікових записів. Встановіть політику блокування облікових записів після певної кількості невдалих спроб входу. Це перешкоджає зловмисникам виконувати безкінечні спроби перебору паролів.
- Затримка перед спробами входу. Додайте затримку перед кожною спробою входу після невдалих спроб. Це ускладнює зловмисникам швидкість перебору паролів і зменшує ймовірність успішної атаки.

- Моніторинг журналу подій. Слідкуйте за журналами подій, особливо за невдалими спробами входу та активностями з підозрілими обліковими записами. Моніторинг допомагає виявити активність brute-force атак і прийняти відповідні заходи.
- Брандмауер та фільтрація трафіку. Використовуйте брандмауери та фільтрацію трафіку для блокування небажаного вхідного трафіку, включаючи спроби brute-force атак. Налаштуйте правила, які обмежують доступ до сервісів, таких як віддалений робочий стіл (RDP), з певних IP-адрес або після певної кількості спроб.
- Оновлення програмного забезпечення; Регулярно оновлюйте операційну систему та програмне забезпечення, оскільки вони можуть містити вразливості, які можуть бути використані для здійснення атак. Оновлення допомагають запобігти використанню відомих вразливостей brute-force атаками.
- Обмеження доступу. Встановіть обмеження доступу до системи тільки з визначених мереж або IP-адрес. Це дозволить вхід тільки з надійних джерел і зменшить ризик небажаних brute-force атак з інших невідомих джерел.
- Повідомлення про спроби атаки. Налаштуйте систему для надсилання повідомлень адміністратору про спроби атаки. Це дозволить оперативно виявляти і реагувати на потенційні brute-force атаки та приймати відповідні заходи безпеки.
- Використання CAPTCHA або рекапчі: Додайте механізм CAPTCHA або рекапчі до важливих точок входу, таких як форми аутентифікації. Це допоможе відрізнити людей від автоматизованих атак і ускладнить зловмисникам виконання brute-force атак.
- Використання інтелектуальних систем виявлення загроз (IDS) і систем захисту від вторгнень (IPS). Встановіть системи, які активно моніторять мережевий трафік та аналізують його на предмет підозрілих дій або вбудованих шаблонів brute-force атак. IDS та IPS можуть автоматично

реагувати на виявлені атаки, наприклад, блокуванням IP-адрес, з яких вони походять.

- Обмеження кількості запитів. Встановіть обмеження на кількість запитів або транзакцій, які можуть бути виконані за певний період часу. Це може ускладнити атакам перебору паролів, обмежуючи кількість спроб за одиницю часу.

Ці загальні методи захисту від brute-force атак можуть бути використані в комбінації для забезпечення максимального рівня безпеки операційної системи і зменшення ймовірності успішної атаки.

2 ЗАХИСТ ВІД BRUTE-FORCE АТАК В ОПЕРАЦІЙНІЙ СИСТЕМІ WINDOWS SERVER 2022

2.1 Огляд операційної системи

Windows Server 2022 є останньою версією серверної операційної системи від Microsoft і пропонує ряд нових функцій та поліпшень, спрямованих на забезпечення безпеки, продуктивності та надійності [3]. Ось загальний огляд деяких ключових функцій та особливостей Windows Server 2022.

Захист інтегрованого мережевого стеку. Windows Server 2022 пропонує покращену захист мережевого стеку з використанням механізмів, таких як "Контроль доступу на основі стану" (Stateful Access Control) та "Постійне правило мережевого екрану" (Persistent Firewall Rule). Це допомагає усунути потенційні вразливості та забезпечити безпеку мережевої комунікації.

Захист від атак на паролі. Windows Server 2022 надає розширені можливості захисту паролів, такі як вимога певної складності пароля та використання політик паролів для встановлення правил використання паролів користувачами. Це допомагає ускладнити процес перебору паролів і підвищує безпеку аутентифікації.

Нові функції віддаленого робочого столу (RDP). Windows Server 2022 пропонує покращені можливості віддаленого робочого столу, включаючи підтримку графічного процесування на віддалених сеансах, покращену продуктивність та забезпечення безпеки через захищену аутентифікацію та шифрування.

Відновлення після збоїв. Windows Server 2022 має покращені можливості відновлення після збоїв, такі як "Миготлива міграція" (Blazing Fast Migration) і "Поступова міграція" (Incremental Migration), що дозволяють зменшити вплив на продуктивність і доступність серверів під час відновлення.

Контейнеризація. Windows Server 2022 пропонує підтримку контейнерів, зокрема "Windows Containers" та "Hyper-V Containers". Це дозволяє розгортання та управління додатками в ізольованих середовищах, що полегшує розробку, тестування та масштабування додатків.

Хмарні інтеграції. Windows Server 2022 підтримує різні хмарні інтеграції, такі як Azure Hybrid Services, що дозволяє легко розширювати інфраструктуру на публічні хмарні сервіси Microsoft Azure та забезпечує більш гнучкі можливості управління та моніторингу.

2.2 Віддалений робочий стіл як об’єкт атаки

2.2.1 Огляд технології віддаленого робочого стола

Віддалений робочий стіл (Microsoft Terminal Services або RDP) є технологією, що дозволяє користувачам підключатися до віддаленого комп'ютера або сервера і працювати з ним так, ніби вони знаходяться перед ним фізично. RDP забезпечує можливість керування віддаленим комп'ютером, виконання програм, доступ до файлів та ресурсів на віддаленому сервері [4].

Основна роль віддаленого робочого стола полягає у забезпеченні зручного та безпечного доступу до даних та ресурсів сервера чи комп'ютера без присутності фізично на місці. Деякі з основних сценаріїв використання RDP включають:

Віддалена адміністрація серверів. RDP дозволяє системним адміністраторам здійснювати віддалене керування серверами без необхідності фізичного присутності у дата-центрі або на місці. Це забезпечує зручність та ефективність управління і підтримки серверної інфраструктури.

Робота з віддаленими робочими станціями. Використання RDP дозволяє користувачам підключатися до своїх робочих станцій або комп'ютерів з будь-якого місця, що дозволяє віддалено працювати зі своїми програмами, файлами та ресурсами. Це особливо корисно для дистанційної роботи, де працівники можуть мати доступ до своїх робочих середовищ з будь-якого місця та пристрою.

Віддалені сесії для спільної роботи. RDP надає можливість віддаленої спільної роботи, де користувачі з різних місць можуть підключатися до одного віддаленого сервера і спільно працювати над проектами, документами або програмами. Це сприяє співпраці і комунікації між віддаленими командами та підприємствами.

RDP відіграє важливу роль у забезпеченні зручного та безпечного доступу до віддалених ресурсів. Він сприяє зручності адміністрування, дистанційної роботи та спільної роботи. Проте, важливо враховувати аспекти безпеки та належно налаштовувати RDP для запобігання можливим загрозам та несанкціонованому доступу.

2.2.2 Brute-force атаки через RDP

Brute-force атаки на Windows Server через віддалений робочий стіл (RDP) є досить поширеним вектором атаки, оскільки RDP дозволяє віддалений доступ до сервера із мережі [5]. Зловмисники можуть спробувати зламати пароль для входу до системи, шляхом автоматизованого перебору всіх можливих комбінацій паролів.

Такі атаки можуть мати серйозні наслідки, якщо зловмисник успішно виконає brute-force атаку і отримає доступ до системи через RDP. Зловмисники можуть отримати доступ до конфіденційної інформації, такої як паролі, корпоративні дані, особисті дані користувачів, віддалений доступ до інших систем і так далі. Це може призвести до порушення приватності, втрати конфіденційності та можливих фінансових збитків. Це може дозволити зловмиснику пошкодити систему, внести зміни в налаштування, встановити шкідливе програмне забезпечення, створити незадокументовані облікові записи або навіть зламати інші системи, підключені до мережі.

Швидка brute-force атака може спричинити перевантаження сервера, що може призвести до відмови в обслуговуванні (DoS) або втрати доступу до ресурсів для легітимних користувачів.

2.3 Методи захисту від brute-force атак

2.3.1 Захист від атак з зовнішньої мережі

Роутер з брандмауером є пристроєм, який виконує функції маршрутизації мережевого трафіку та забезпечує захист мережі шляхом встановлення правил

фільтрації трафіку. Він виконує роль важливого компонента в мережевій інфраструктурі, дозволяючи підключати комп'ютери та інші пристрої до Інтернету та інших мереж [5].

Роутер з функцією брандмауера має декілька основних функцій, які сприяють захисту Windows Server від brute-force атак по RDP.

Маршрутизація.

Роутер забезпечує передачу мережевого трафіку між різними мережами, включаючи локальну мережу, в якій знаходиться Windows Server, та зовнішню мережу, як, наприклад, Інтернет. Це дозволяє контролювати шляхи, по яких проходить трафік з мережі Інтернет, та унеможливлює прямий доступ до сервера ззовні.

Брандмауер.

Брандмауер в роутері дозволяє фільтрувати мережевий трафік, блокуючи небажаний або потенційно шкідливий трафік. Він може мати правила, які контролюють доступ до певних портів та протоколів, включаючи порти, які використовуються для RDP. Це дозволяє обмежити можливість зовнішнього доступу до RDP-служби сервера та зменшити потенційну загрозу brute-force атак.

NAT.

Роутер може виконувати функцію NAT, яка перетворює приватні IP-адреси в публічні IP-адреси та навпаки. Це забезпечує анонімність локальної мережі, оскільки зовнішні пристрої не можуть прямо підключитися до приватних IP-адрес комп'ютерів в мережі. Це ще один шар захисту, який допомагає унеможливити прямі атаки на Windows Server через RDP.

VPN.

Роутер може підтримувати функцію VPN, яка дозволяє створювати безпечне з'єднання між віддаленими користувачами та локальною мережею. Використання VPN забезпечує шифрування трафіку та автентифікацію користувачів, зменшуючи ризик небажаного доступу до RDP-сервісу через Інтернет.

Ці функції роутера з брандмауером сприяють захисту Windows Server від brute-force атак по RDP, обмежуючи доступ до RDP-служби зовнішніх користувачів та фільтруючи небажаний трафік. Проте важливо налагодити правильні правила фільтрації трафіку в роутері та регулярно оновлювати його програмне забезпечення, щоб забезпечити максимальний рівень безпеки.

Схема підключення корпоративної мережі до мережі Інтернет через роутер з брандмауером показана на рисунку 2.1

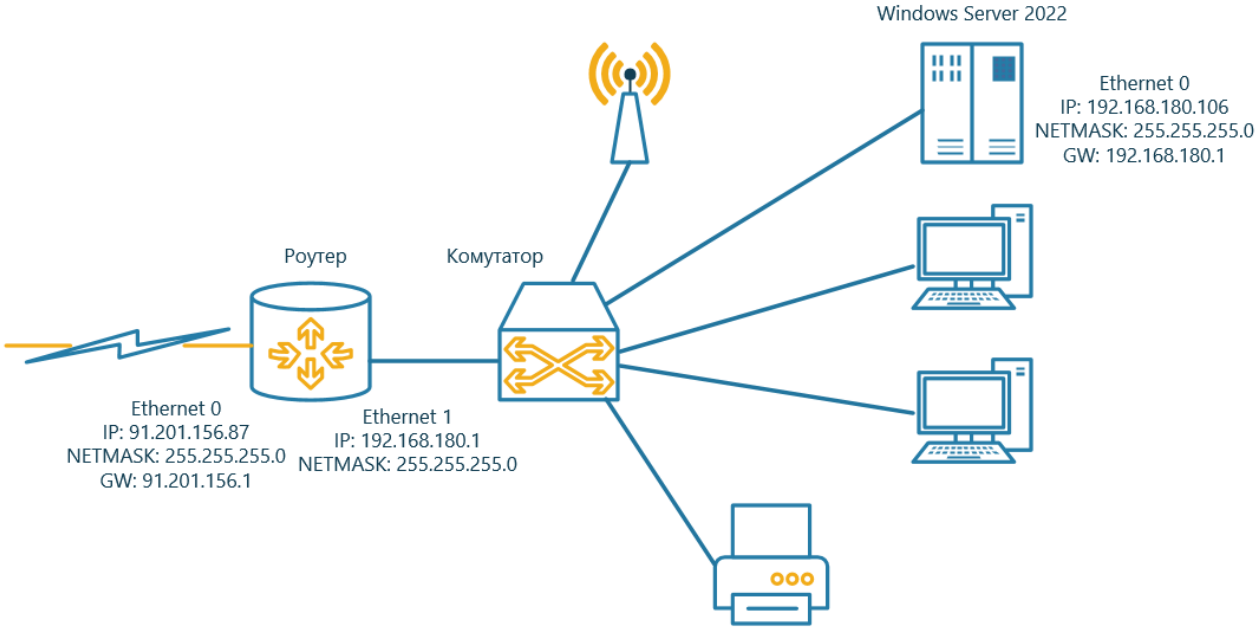

Рисунок 2.1 – Схема підключення корпоративної мережі до мережі Інтернет

Корпоративна мережа - це внутрішня локальна мережа, де знаходяться комп'ютери, сервери та інші пристрої, що використовуються в організації. Ця мережа має внутрішню IP-адресацію і використовувати приватні IP-адреси з мережі 192.168.180.0/24, які не є доступними з Інтернету.

Роутер є точкою підключення між корпоративною мережею та зовнішньою мережею Інтернет. Він повинен мати не менше двох мережевих інтерфейсів – один Ethernet 1, що підключений до корпоративної мережі, інший Ethernet 0 - до зовнішньої мережі. Роутер повинен мати вбудований брандмауер, який контролює трафік, що проходить через нього. Брандмауер дозволяє встановлювати правила фільтрації трафіку для обмеження доступу до певних

портів, протоколів або IP-адрес. Також роутер виконує функцію NAT, яка перетворює приватні IP-адреси корпоративної мережі на публічні IP-адреси, які доступні з Інтернету. Це забезпечує анонімність та безпеку локальної мережі.

Додаткові заходи безпеки, такі як використання віртуальних приватних мереж (VPN), можуть бути реалізовані для забезпечення безпечного зовнішнього доступу до корпоративної мережі через роутер.

Ця схема підключення та фільтрації трафіку допомагає забезпечити безпеку Windows Server від brute-force атак по RDP з мережі Інтернет, обмежуючи доступ до RDP-служби зовнішніх користувачів та контролюючи трафік, що входить і виходить з мережі. Однак, важливо правильно налаштувати роутер та брандмауер, встановити відповідні правила фільтрації трафіку та регулярно оновлювати їх, щоб забезпечити максимальний рівень захисту.

В якості роутера можуть використовуватися спеціалізовані пристрої від виробників, таких як Cisco або Mikrotik. Ці пристрої зазвичай мають розширені функціональні можливості, які дозволяють налаштовувати безпеку, фільтрацію трафіку та інші параметри забезпечення мережі.

Також можливе використання роутерів на базі операційних систем Unix або Linux, наприклад, з використанням операційної системи FreeBSD. FreeBSD є надійною та стабільною платформою, яка може виконувати функції роутера та брандмауера. Вона має багатий набір інструментів, які дозволяють налаштовувати політики безпеки, фільтрацію трафіку, VPN та інші аспекти захисту мережі.

На рисунку 2.2 показано приклад налаштування правил брандмауер на обладнанні Mikrotik.

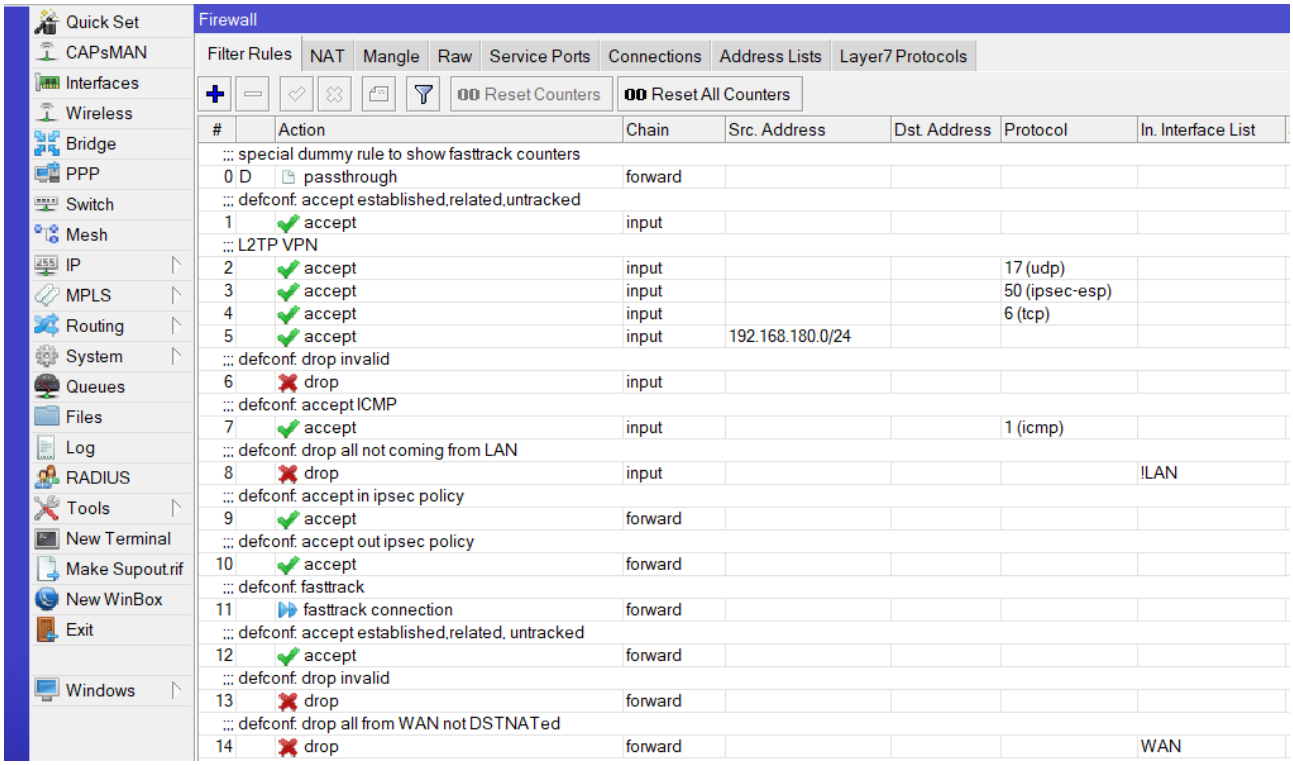

Рисунок 2.2 – Налаштування правил брандмауера на обладнанні Mikrotik

На рисунку 2.3 показано приклад налаштування правил NAT на обладнанні Mikrotik.

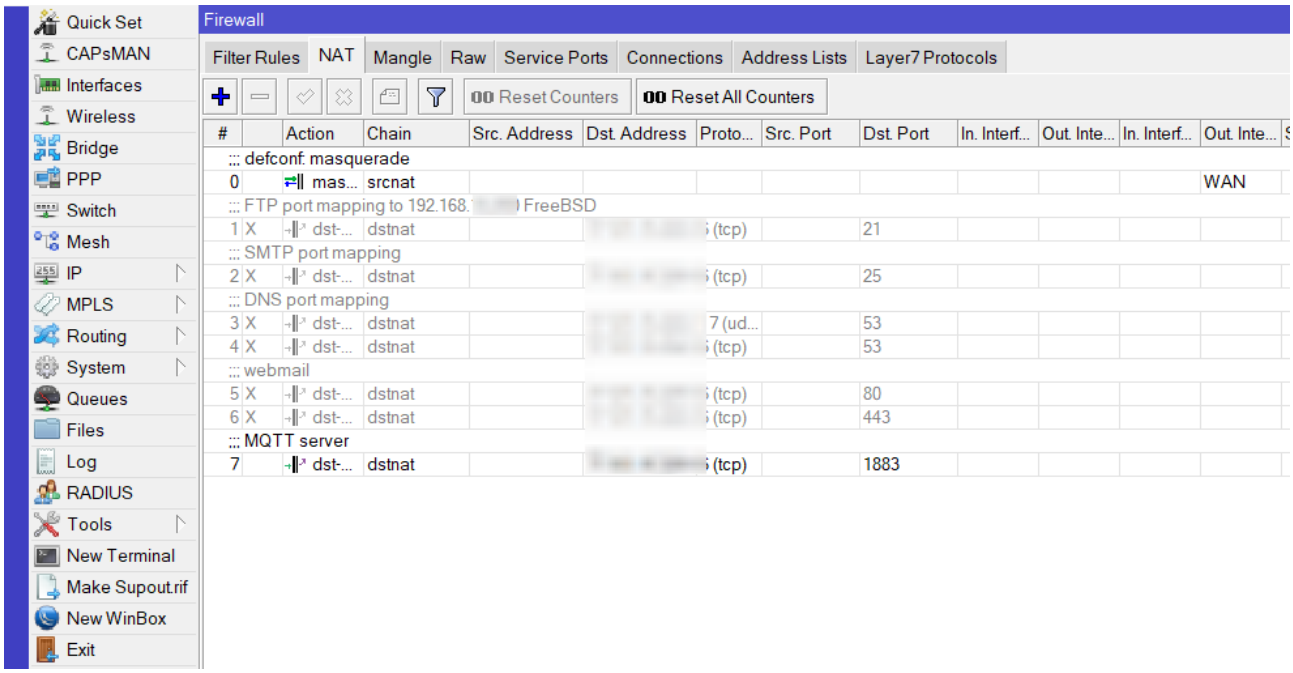

Рисунок 2.3 – Налаштування правил NAT на обладнанні Mikrotik

Вибір конкретного роутера та операційної системи для роутера залежить від потреб і вимог вашої організації, а також від розмірів мережі та рівня безпеки, який ви хочете досягти. Важливо обрати надійне обладнання або платформу з належними функціональними можливостями та підтримкою безпеки, а також

мати достатні знання та досвід для правильного налаштування та управління ними.

2.3.2 Захист від атак з локальної мережі.

Захист від brute-force атак з локальної мережі є важливою складовою безпеки корпоративної інфраструктури.

В Windows Server 2022 вбудовані різноманітні механізми захисту від brute-force атак, включаючи політики паролів. Політики паролів визначають правила та вимоги щодо створення та використання паролів користувачами [6]. Ось деякі основні аспекти політики паролів і їх вплив на захист від brute-force:

1) Складність паролів. Політика паролів повинна вимагати використання складних паролів, які містять комбінацію великих і малих літер, цифр та спеціальних символів. Це збільшує кількість можливих комбінацій і ускладнює завершення успішної brute-force атаки.
2) Мінімальна довжина паролів. Політика може встановлювати мінімальну довжину пароля, наприклад, вимагати, щоб пароль був не менше 8 або 10 символів у довжину. Це змушує користувачів використовувати більш довгі паролі, що зменшує ефективність brute-force атак.
3) Періодична зміна паролів. Політика паролів може вимагати періодичної зміни паролів користувачами, наприклад, кожні 30, 60 або 90 днів. Це запобігає використанню старих та вже скомпрометованих паролів, зменшуючи ризик успішних brute-force атак.
4) Блокування після невдалих спроб. Політика блокування облікових записів користувачів може встановлювати обмеження на кількість невдалих спроб введення пароля перед блокуванням облікового запису користувача. Наприклад, після 5 невдалих спроб може бути автоматично заблоковано обліковий запис на певний період часу. Це ускладнює проведення brute-force атаки, оскільки зловмиснику доведеться швидко зламати пароль у вузькому вікні часу.

5) Історія паролів. Політика паролів може зберігати історію попередніх паролів користувачів, щоб уникнути повторного використання тих же самих паролів. Це запобігає зловмисникам повторно використовувати раніше скомпрометовані паролі при brute-force атаках.

На рисунку 2.4 показано налаштування політики паролів в операційній системі Windows Server 2022 в консоль редактора групової політики.

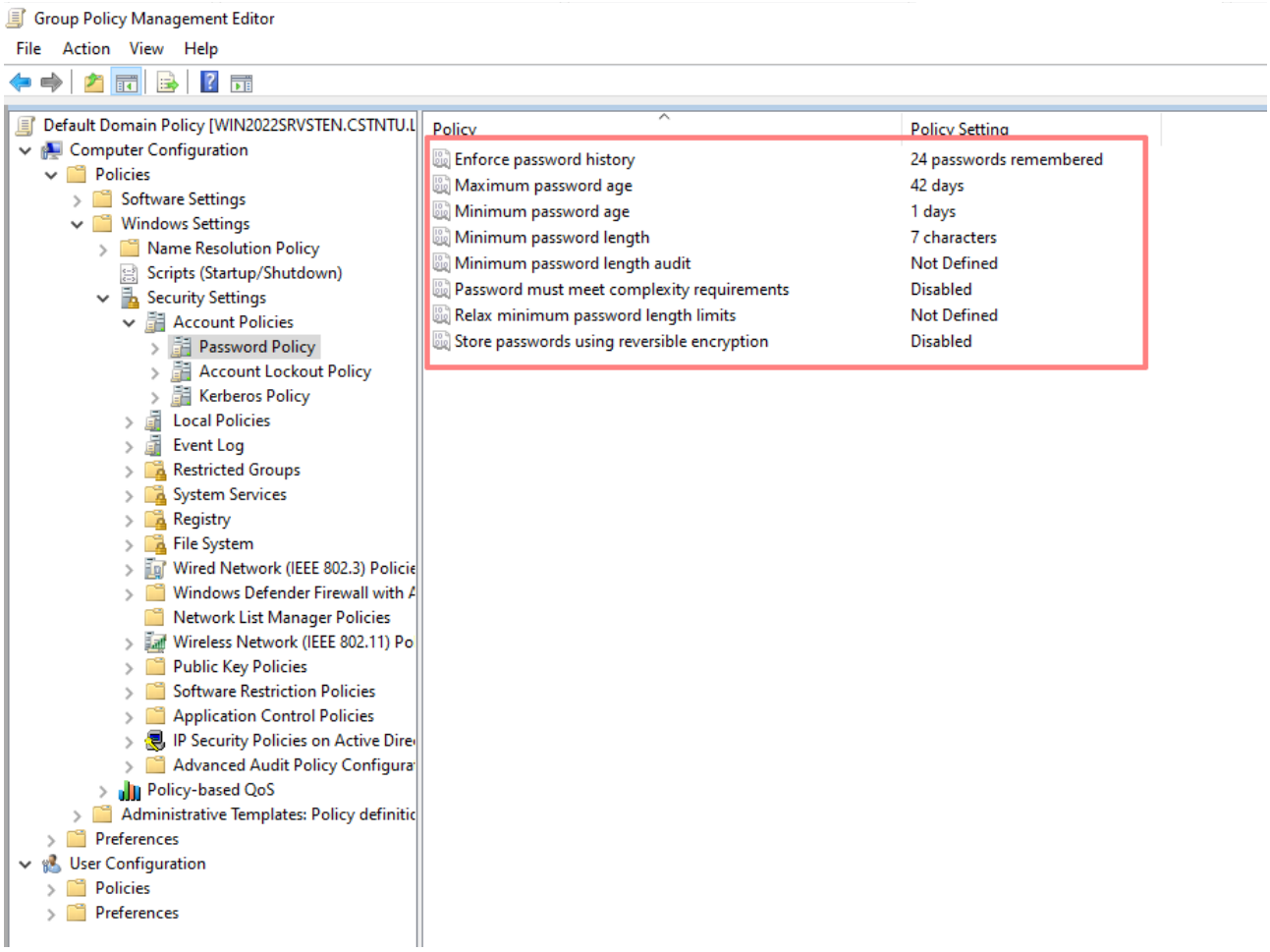

Рисунок 2.4 – Налаштування політики паролів в операційній системі Windows Server 2022

На рисунку 2.5 показано налаштування політики блокування облікових записів користувачів в операційній системі Windows Server 2022 в консоль редактора групової політики [7].

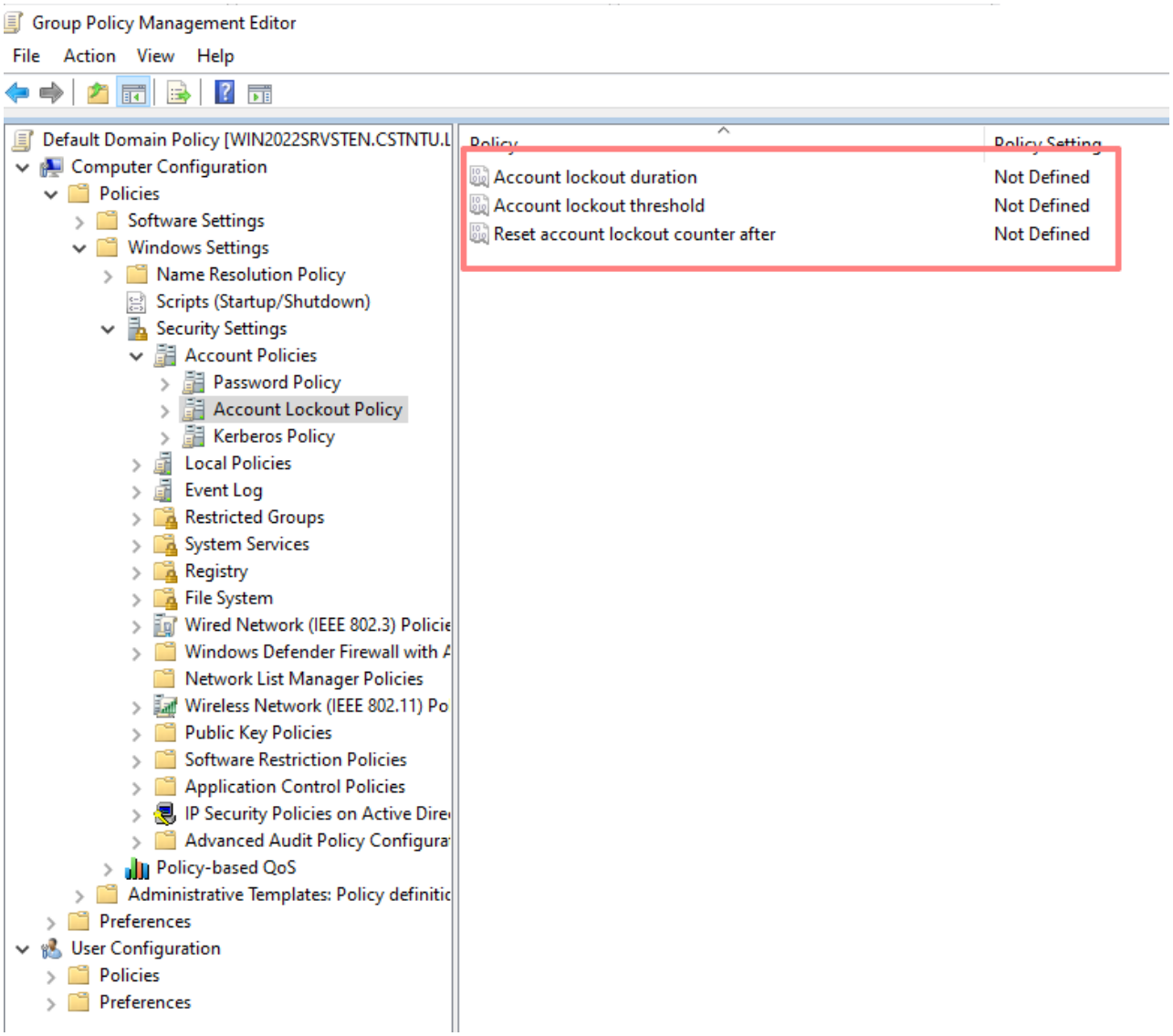

Рисунок 2.5 – Налаштування політики блокування облікових записів користувачів в операційній системі Windows Server 2022

Всі ці механізми спільно допомагають підвищити рівень захисту від brute-force атак в Windows Server. Однак важливо налаштувати їх належним чином та постійно оновлювати систему з метою забезпечення найвищого рівня безпеки.

2.4 Здійснення brute force атаки на RDP -сервер

Brute-force атака на RDP-сервер - це спроба отримати несанкціонований доступ до системи шляхом послідовного перебору всіх можливих комбінацій користувачів та паролів. У контексті RDP це означає спроби зламати пароль для доступу до віддаленого робочого столу сервера.

Рисунок 2.6 показує структурну схему мережі, яка буде використана для здійснення brute force атаки на RDP-сервер.

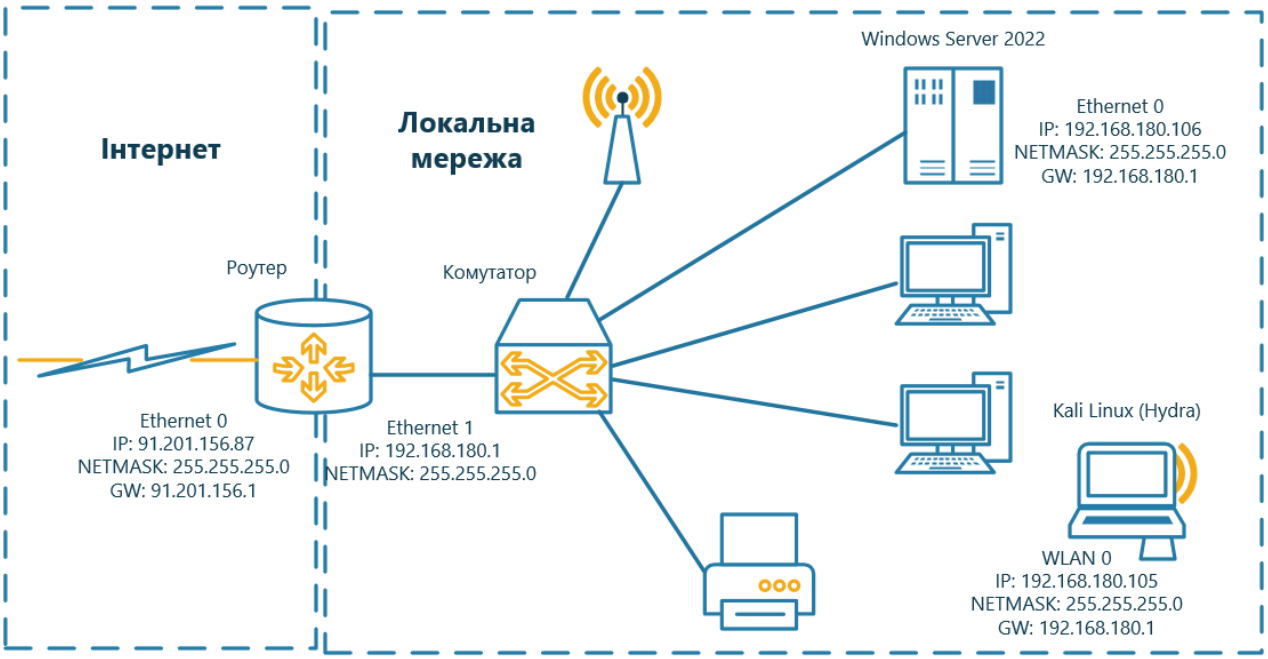

Рисунок 2.6 – Схема мережі для проведення brute-force атаки на RDP-сервер

Схема мережі для атаки включає наступні компоненти:

1) Клієнтський комп'ютер. Це комп'ютер, на якому встановлено відповідні інструменти для здійснення атаки. Цей комп'ютер використовується для запуску атаки та надсилання запитів до RDP-сервера та має IP 192.168.180.105.

2) Windows Server з RDP. Це цільовий сервер, на якому запущено службу віддаленого робочого столу (Microsoft Terminal Services). Цей сервер використовується для отримання з'єднання від клієнтського комп'ютера та надання доступу до віддаленого робочого столу та має IP 192.168.180.106.

3) Локальна мережа. Це мережа, в якій знаходяться клієнтський комп'ютер і RDP-сервер.

В цій схемі мережі клієнтський комп'ютер виконує brute force атаку на RDP-сервер, який знаходиться в локальній мережі. Клієнтський комп'ютер і RDP-сервер спілкуються через мережу, і атакуючий надсилає послідовно комбінації користувачів та паролів до RDP-сервера з метою підбору пароля і отримання доступу.

Добавимо користувача Admin з паролем 123456 в операційну систему Windows Server 2022 (Рис.2.7).

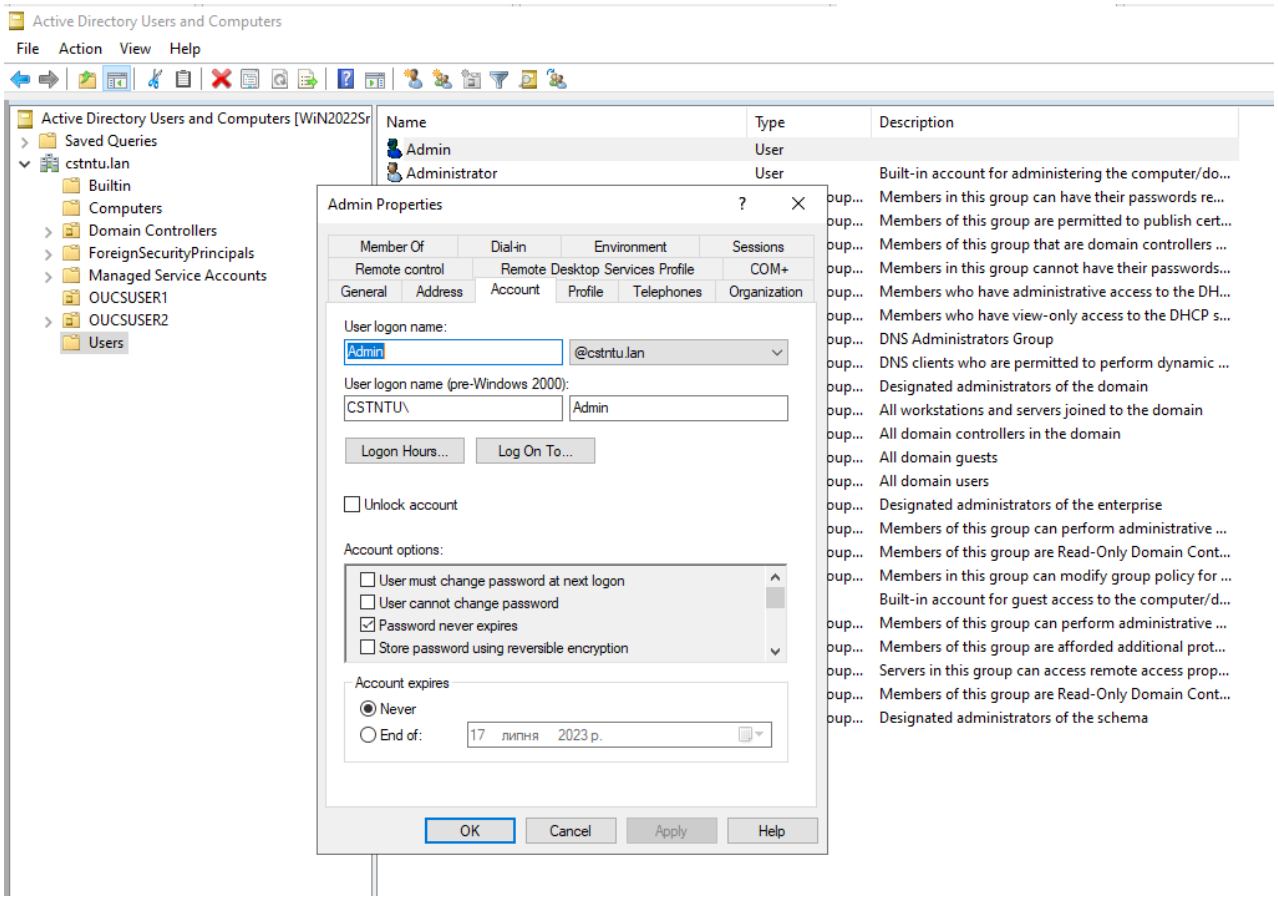

Рисунок 2.7 – Створення користувача Admin в Windows Server 2022

На даному етапі тестування Window Server не застосовує політику паролів та політику блокування облікових записів.

Для показу методики проведення brute-force використаємо Kali Linux та інструмент Hydra.

Kali Linux - це спеціалізована операційна система заснована на Debian, яка має в своєму складі набір інструментів для тестування безпеки мереж та здійснення різних типів атак. Вона широко використовується пентестерами та етичними хакерами для проведення різноманітних тестів на проникнення [8].

Hydra - це один з інструментів, доступних в Kali Linux, який спеціалізується на здійсненні brute-force атак на різноманітні протоколи, включаючи RDP. Він працює шляхом надсилання послідовних запитів до сервера з різними комбінаціями користувачів та паролів з метою підбору логіна та пароля і отримання несанкціонованого доступу [9].

Brute-force атака на RDP-сервер за допомогою Hydra включає наступну послідовність кроків:

1) Збір інформації. Першим кроком є збір необхідної інформації про цільовий RDP-сервер. Для збору інформації використаємо утиліту nmap в Kali Linux.

Nmap - це популярний і потужний інструмент для сканування мережі і виявлення хостів, портів, сервісів та інших відомостей про системи в мережі. Він широко використовується в області мережевої безпеки та тестування на проникнення.

У Kali Linux Nmap вже встановлений за замовчуванням, оскільки це спеціалізований дистрибутив для тестування на проникнення.

Введемо в терміналі Kali Linux наступну команду.

```
#nmap -sC -sV 192.168.180.106 -Pn
```

де:

- `-sC` - вказує від Nmap виконувати скриптову верифікацію. Це дозволяє виконувати певні скрипти, які допомагають виявити вразливості або збір інформації про сервіси на цільовому хості;
- `-sV` - вимагає від Nmap виявляти версії сервісів, які працюють на відкритих портах. Вона дозволяє отримати більше інформації про сервіси, що запущені на хості;
- `-Pn` - вимагає від Nmap сканувати хост, не виконуючи перевірку доступності за допомогою ICMP. Це корисно, якщо фільтрація ICMP пакетів відбувається на цільовому хості або якщо ви хочете уникнути виявлення Nmap через ICMP протокол;

В даному випадку команда виконує сканування портів і виконує скриптову верифікацію на хості з IP-адресою 192.168.180.106 без відправки ICMP пакетів.

В результаті роботи сканер nmap успішно виявлено RDP сервер на порті 3389/tcp (Рис.2.8).

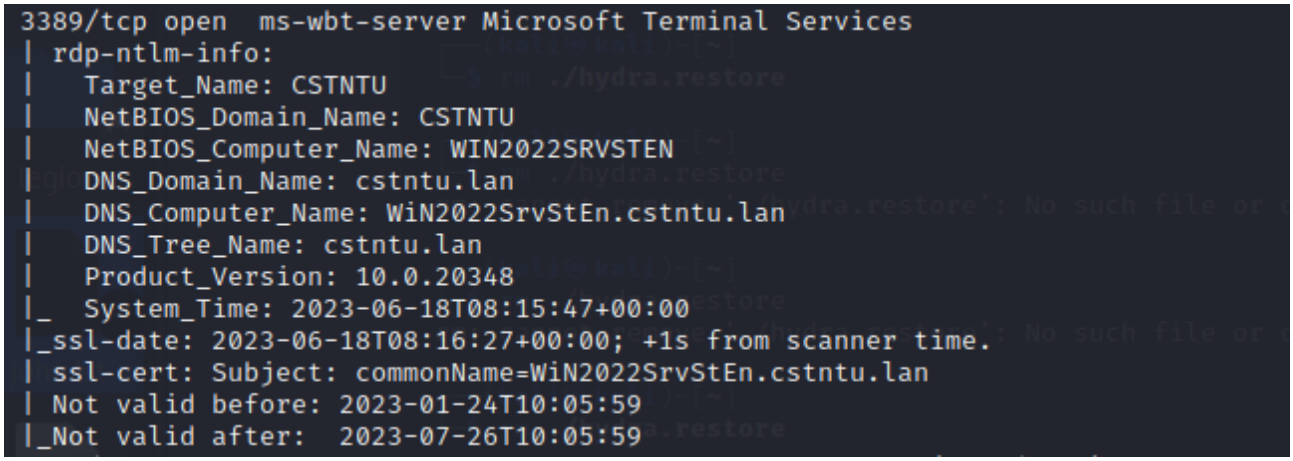

Рисунок 2.8 – Результати роботи сканера nmap

Також можуть бути зібрані додаткові дані, які можуть допомогти в атаці, наприклад, список можливих користувачів або попередньо визначені паролі.

2) Налаштування Hydra. Далі потрібно налаштувати Hydra для здійснення атаки на RDP-сервер. Це включає визначення протоколу (RDP), цільової IP-адреси, порту та списку можливих комбінацій користувачів та паролів.

Використаємо консольну команду hydra для запуску атаки грубої сили на RDP-сервер. Нижче наведений загальний синтаксис команди.

`hydra -t 1 -V -l <логін> -P <шлях-до-файлу-з-паролями> rdp://<IP-адреса-RDP-сервера>`

У цій команді:

- `-t 1` - вказує, що використовуватиметься лише один потік (одночасна спроба входу) для маскування спроб підбору пароля;

- `-V` - включає режим показу більш детальної інформації під час атаки;

- `-l <логін>` - вказує логін, який буде перевірятися під час атаки;

- `-P <шлях-до-файлу-з-паролями>` - вказує шлях до файлу, який містить список паролів, що будуть перевірятися під час атаки;

- `rdp://<IP-адреса-RDP-сервера>` - вказує адресу RDP-сервера, до якого ви хочете отримати доступ.

3) Запуск атаки. Після введення команди Hydra почне виконувати атаку грубої сили на RDP-сервер, перевіряючи різні комбінації логінів та паролів з вказаного файлу. Якщо успішний варіант логіна та пароля буде знайдений, Hydra повідомить про це.

За результатами атаки можна зробити висновок, що процес підбору пароля був успішним. Це підтверджується рисунком 2.9.

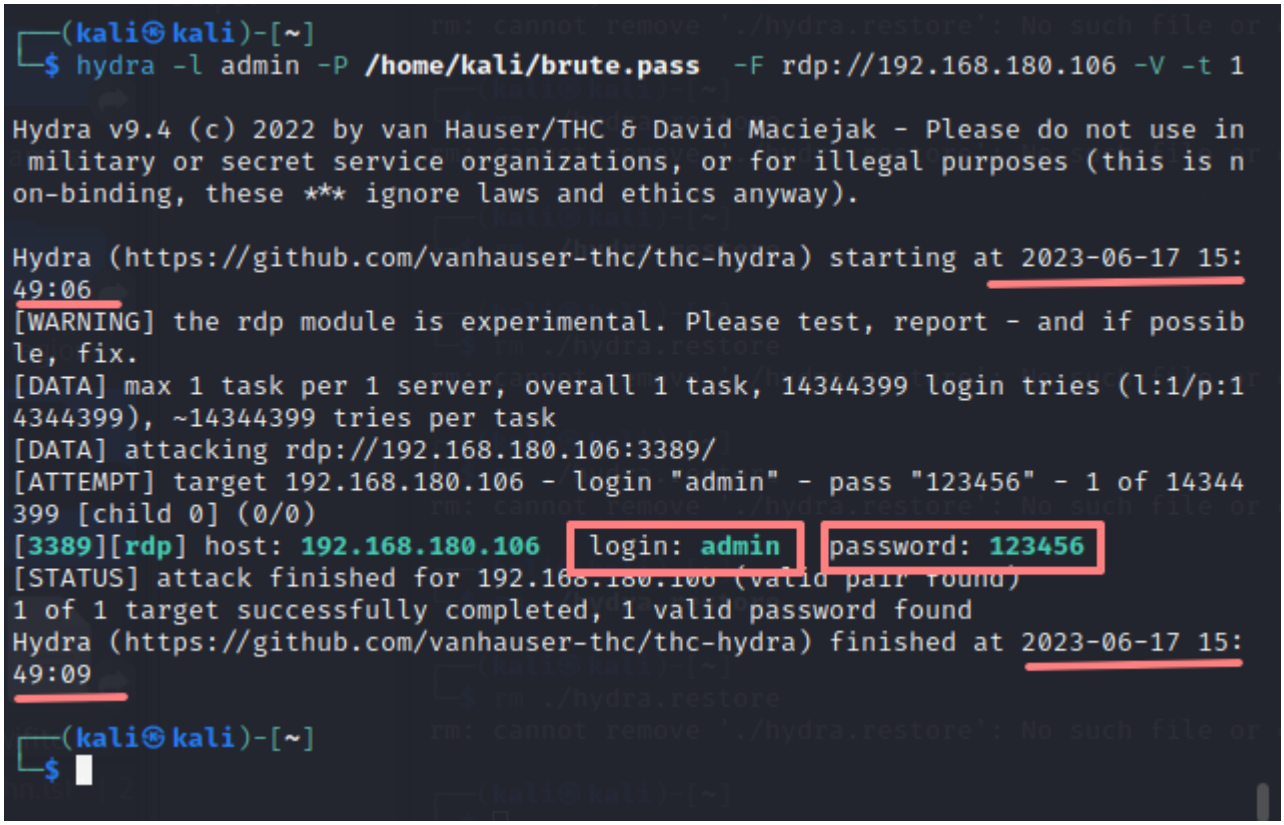

Рисунок 2.9 – Результати проведення brute-force атаки на RDP-сервер

Встановлений пароль 123456 для користувача admin був відгаданий вкрай швидко. Тому що ця brute-force атака була проведена з використанням встановленого простого пароля та явно вказаного імені користувача в параметрах запуску Hydra. При реальній атаці грубої сили на RDP-сервери потрібна велика кількості комбінацій для підбору паролів, що може зайняти тривалий час.

2.5 Встановлення політики облікових записів

Як вже було сказано в п.2.3.2 в Windows Server 2022 є вбудовані механізми захисту від brute-force атак, включаючи політику паролів та політику блокування облікових записів користувачів.

Політики паролів (Password Policies) - це набір правил та вимог, які встановлюються для створення та використання паролів облікових записів

користувачів в операційній системі. Ці політики визначають параметри, які обмежують характеристики паролів, такі як довжина, складність, термін дії та інші вимоги безпеки [6].

Основна мета політик паролів полягає в забезпеченні безпеки облікових записів користувачів шляхом використання сильних та надійних паролів. Вони допомагають запобігти атакам грубої сили (brute-force) та зменшують ризик несанкціонованого доступу до системи через вгадування або перебір паролів.

Встановлення ефективних політик паролів допомагає підвищити безпеку системи, запобігти несанкціонованому доступу та зберегти конфіденційність облікових записів користувачів.

Політика блокування облікових записів користувачів (Account Lockout Policy) - це набір правил та налаштувань, які визначають умови, за яких обліковий запис користувача буде заблоковано після певної кількості невдалих спроб аутентифікації [7].

Ця політика використовується для запобігання атакам грубої сили (brute-force) та зловживанню, коли хтось намагається незаконно отримати доступ до облікових записів, шляхом послідовного перебору можливих паролів.

Зазвичай політика блокування облікових записів встановлює кількість дозволених невдалих спроб входу, після чого обліковий запис блокується на певний час.

Налаштування політики блокування облікових записів дозволяє забезпечити додатковий рівень безпеки, зменшити ризик успішних атак brute-force та зберегти цілісність та конфіденційність облікових записів користувачів.

Активуємо та налаштуємо дані політики на Windows Server 2022.

На рисунку 2.10 показано налаштування та застосування політики паролів в операційній системі Windows Server 2022 в консоль редактора групової політики.

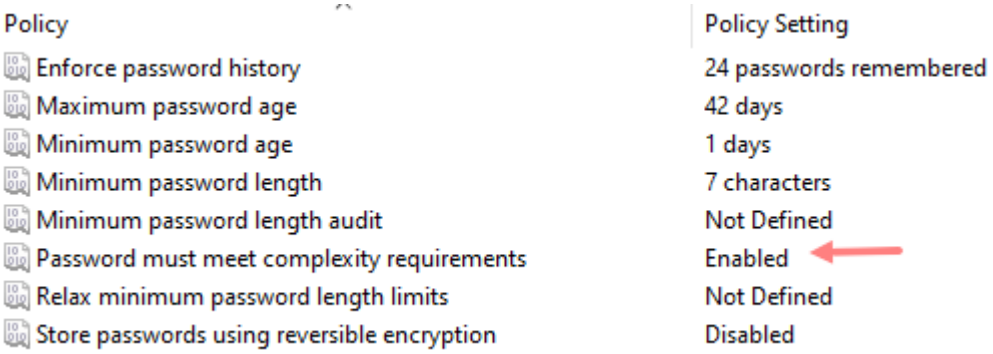

Рисунок 2.10 – Налаштування та застосування політики паролів

де:

1) `Enforce password history - 24 passwords remembered` – означає, що система буде запам'ятовувати останні 24 використані паролі користувача і не дозволить повторно використовувати їх. Це допомагає запобігти використанню старих паролів, що може зробити облікові записи більш безпечними;
2) `Maximum password age - 42 days` - цей параметр вказує на максимальний термін дії паролю. Після цього терміну користувачеві буде потрібно змінити свій пароль. Встановлення максимального строку дії допомагає підтримувати актуальність паролів та зменшує ризик їхнього скомпрометування;
3) `Minimum password age - 1 days` - це поле вказує мінімальний термін, протягом якого користувач повинен зберігати свій пароль перед зміною. Встановлення цього параметра може запобігти користувачам часто змінювати паролі, щоб повернутись до свого попереднього паролю;
4) `Minimum password length - 7 characters` – це встановлює мінімальну довжину паролю, яку має використовувати користувач. Встановлення достатньої довжини допомагає ускладнити процес відгадування паролю і забезпечує вищий рівень безпеки;
5) `Minimum password length audit - Not Defined` – цей параметр визначає, чи слід перевіряти відповідність мінімальній довжині паролів при аудиті безпеки;
6) `Password must meet complexity requirements – Enabled` – ей параметр вимагає, щоб пароль мав складність і включав різноманітні

елементи, такі як великі та малі літери, цифри та спеціальні символи. Це сприяє створенню паролів, які складніше відгадати або підібрати;

7) `Relax minimum password length limits - Not Defined` – цей параметр визначає, чи слід зменшувати обмеження на мінімальну довжину паролів для певних користувачів або груп.
8) `Store passwords using reversible encryption – Disabled` – цей параметр визначає, чи слід зберігати паролі з використанням оборотного шифрування. Вимкнення цього параметра є рекомендованим, оскільки зберігання паролів у формі, зворотній до шифрування, може представляти загрозу безпеці.

На рисунку 2.11 показано налаштування та застосування політики блокування облікових записів користувачів в операційній системі Windows Server 2022 в консоль редактора групової політики.

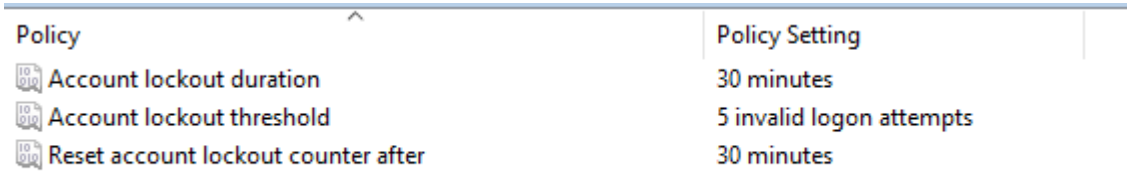

Рисунок 2.11 – Налаштування та застосування політики блокування облікових записів користувачів

де:

1) `Account lockout duration - 30 minutes` – цей параметр визначає, як довго обліковий запис буде заблокований після досягнення порогового значення невірних спроб входу. У цьому випадку, після заблокування облікового запису, він буде розблокований автоматично через 30 хвилин;
2) `Account lockout threshold - 5 invalid logon attempts` – цей параметр вказує на кількість невірних спроб входу, після яких обліковий запис буде заблоковано. У цьому випадку, якщо користувач здійснить 5 невірних спроб входу, його обліковий запис буде заблоковано;
3) `Reset account lockout counter after - 30 minutes` – цей параметр визначає період часу, після якого лічильник невірних спроб входу буде

скинутий. У даному випадку, після 30 хвилин без невірних спроб входу, лічильник буде скинутий і користувач зможе знову використовувати свій обліковий запис.

Змінимо пароль користувача Admin згідно встановлених вимог політики паролів та повторно здійснимо brute-force атаку.

Як можна побачити з рисунку 2.12 підбір паролю користувача пройшов невдало.

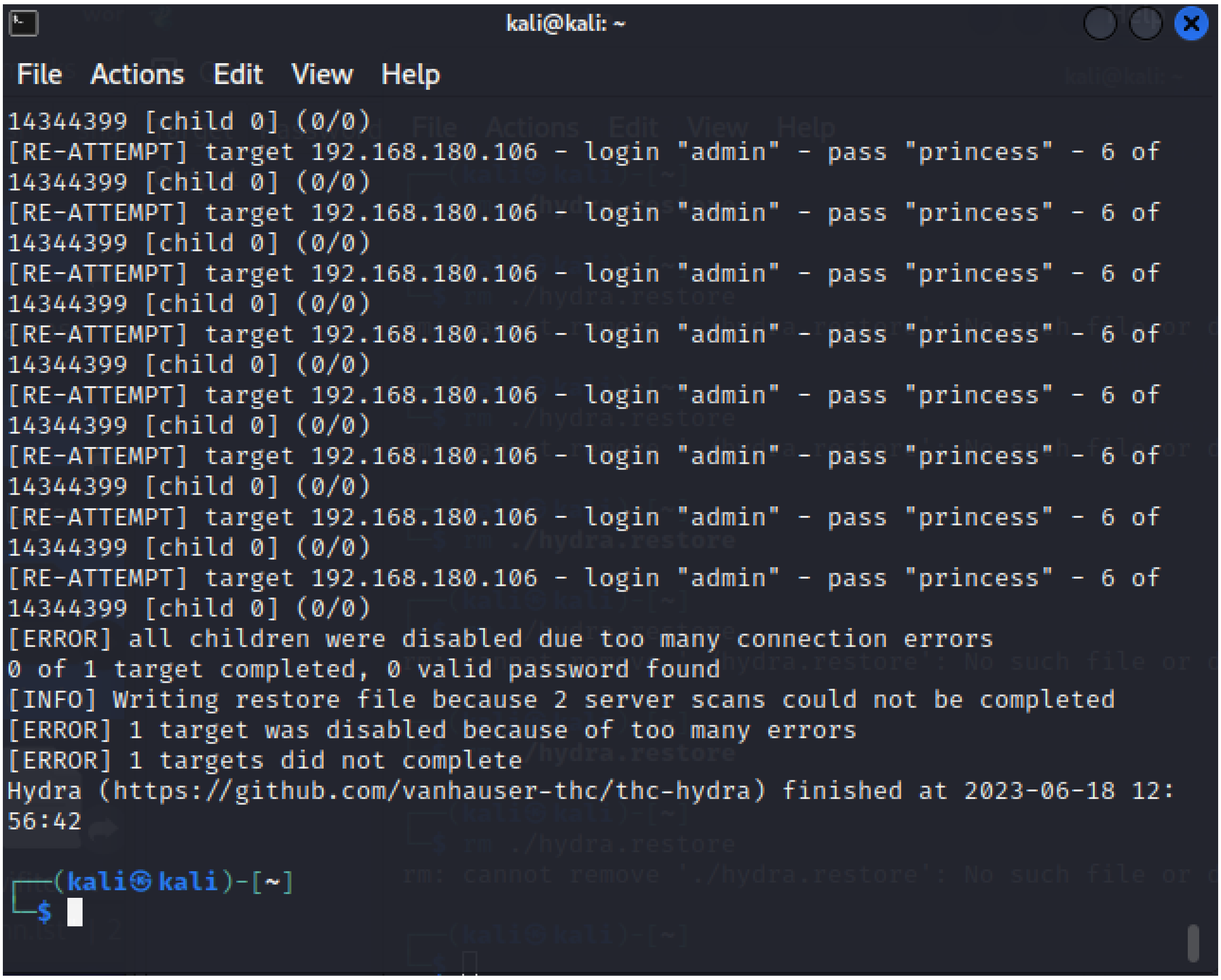

Рисунок 2.12 – Невдала спроба brute-force атаки при застосуванні політики блокування облікових записів користувачів

Якщо атакуючий виконує багато невірних спроб входу і перевищує порогове значення, визначене політикою блокування, обліковий запис буде автоматично заблокований (Рис.2.13). Це зупинило подальші спроби входу і відповідно здійснення brute-force атаки.

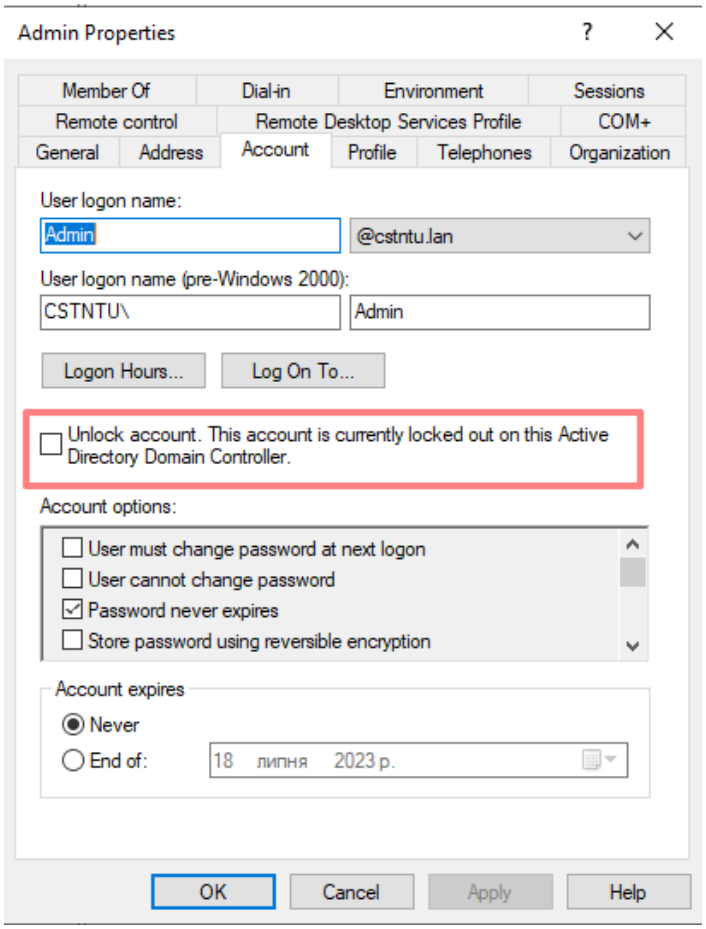

Рисунок 2.13 – Заблокований обліковий запис користувача Admin

Ці політики дозволяють забезпечити високий рівень безпеки паролів і ускладнюють процес зламу акаунтів методом brute-force.

Але коли обліковий запис заблоковано, користувач не зможе увійти, навіть якщо введе правильний пароль. Це є великою проблемою в корпоративній мережі. Оскільки це призводить до перешкод у роботі користувачів і зниженні продуктивності праці. Блокування облікових записів після кількох невдалих спроб входу як правило є неефективним та викликає додаткові проблеми. Щоб запобігти блокуванню облікових записів при brute-force атаці не вимикаючи сам механізм блокування потрібно розробити механізм блокування IP адрес зловмисників. Даний механізм має спрацьовувати до блокування облікових записів користувачів.

3 РОЗРОБКА ТА ТЕСТУВАННЯ СИСТЕМИ АВТОМАТИЧНОГО БЛОКУВАННЯ IP-АДРЕС ЗЛОВМИСНИКІВ

3.1 Розробка системи автоматичного блокування IP зловмисника

Система автоматичного блокування IP-адрес зловмисників є надзвичайно важливою при боротьбі з brute-force атаками. Ось кілька причин, чому це має велике значення:

1) Запобігання несанкціонованому доступу. Brute-force атаки спрямовані на відгадування паролів шляхом послідовного перебору всіх можливих комбінацій. Це може призвести до успішного злому системи і несанкціонованого доступу до конфіденційних даних. Система автоматичного блокування IP-адрес дозволяє виявляти такі атаки і негайно блокувати IP-адреси зловмисників. Це ефективно запобігає успішним brute-force атакам і забезпечує безпеку системи.
2) Ефективне використання ресурсів. Автоматичне блокування IP-адрес зловмисників допомагає економити ресурси операційної системи. Враховуючи те, що brute-force атаки можуть бути дуже інтенсивними, швидка реакція і блокування IP-адрес зменшують навантаження на обчислювальні ресурси. Це сприяє покращенню продуктивності та доступності системи для законних користувачів.
3) Попередження майбутніх атак. Система автоматичного блокування IP-адрес не тільки буде реагувати на поточні brute-force атаки, але й буде надавати дані для подальшого аналізу. Шляхом моніторингу та реєстрації заблокованих IP-адрес, можна виявити шаблони, поведінку зловмисників і вдосконалити заходи безпеки. Це допомагає зрозуміти характеристики атак і підвищити ефективність системи захисту.

Розробка системи автоматичного блокування IP-адрес зловмисника є необхідною для ефективного захисту від brute-force атак. Ця система буде запобігати несанкціонованому доступу, здійснювати захист від перебору

паролів, сприяти ефективному використанню ресурсів системи та надавати можливість аналізу для подальшого вдосконалення заходів безпеки.

3.1.1 Огляд можливостей PowerShell

Написання програмного модуля автоматичного блокування IP-адрес зловмисників буде зроблено на PowerShell [10].

PowerShell - це мова сценаріїв та інтерактивна оболонка командного рядка, розроблена компанією Microsoft. Вона спеціально створена для автоматизації завдань та управління системами, зокрема операційною системою Windows.

PowerShell базується на платформі .NET Framework та надає доступ до широкого спектру функцій інтегрованого середовища Windows, включаючи доступ до об'єктів системи, служб, реєстру, файлової системи, мережі та багато іншого. Вона дозволяє виконувати скрипти для автоматизації повсякденних завдань, таких як управління конфігурацією, моніторинг системи, обробка даних, налаштування мережі та безпеки, взаємодія зі службами та додатками, аналіз журналів подій та багато іншого.

PowerShell використовується як інструмент для автоматизації завдань системного адміністрування, розробки програмного забезпечення, тестування, налагодження, аналізу даних та інших сценаріїв. PowerShell є потужним інструментом для адміністрування Windows Server, налаштування безпеки, моніторингу системи, автоматизації рутинних завдань та багато іншого. Вона надає доступ до широкого спектру команд та модулів, що дозволяє ефективно управляти серверами і розширювати їх можливості.

3.1.2 Написання сценарію PowerShell

Напишемо сценарій PowerShell, який буде аналізувати журнал подій заблокованих спроб авторизації (Event ID 4625) за останні 10 хвилин. Потім сценарій буде підраховувати кількість невдалих спроб авторизації для кожної IP-адреси. Якщо кількість невдалих спроб перевищуватиме поріг (у нашому

випадку 5), сценарій буде автоматично створювати правило блокування додавати IP-адреси в вбудованому брандмауері Windows Server 2022.

На рисунку 3.1 показано даний сценарій з роз'ясненням кожного рядка.

blockIPbruteforce1minServer2.ps1

```powershell
# створюємо змінну, яка містить час, відносно якого будемо шукати спроби підбору паролів.
#
$Set_Last_Minutes = [DateTime]::Now.AddMinutes(-10)
#
# назву журналу подій, з якого  будемо отримувати інформацію про спроби підбору паролів.
#
$LogName = "Security"
#
# Ця частина коду отримує події з журналу подій "Security", які мають ID 4625 (невдалий вхід в систему)
# та тип входу "3" (вхід через RDP). Фільтруємо ці події із застосуванням поточного часу та обмеженням останніх 10 хвилин.
# Також вибираємо IP-адресу з цих подій та зберігаємо її у змінній $badRDPlogons.
#
$badRDPlogons = Get-WinEvent -FilterHashtable @{
    LogName = $LogName
    StartTime = $Set_Last_Minutes
    ID = 4625
} | Where-Object { $_.Message -match 'logon type:\s+(3)\s' } | Select-Object @{n='IpAddress';e={$_.Properties[19].Value}}
#
# Цей рядок групує IP-адреси зі змінної $badRDPlogons і обирає ті, що мають більше 5 спроб підбору паролів.
# Ми зберігаємо ці IP-адреси у змінній $getip.
#
$getip = $badRDPlogons | Group-Object -Property IpAddress | Where-Object {$_.Count -gt 5} | Select-Object -Property Name
#
# Цей рядок встановлює шлях до лог-файлу, куди будуть записуватися інформація про заблоковані IP-адреси.
#
$log = "C:\Bruteforce\blocked_bruteforce_ip.txt"
#
# У цій частині проходимо через кожну IP-адресу зі змінної $getip.
# Для кожної IP-адреси генеруємо назву правила брандмауера, видаляємо це правило (якщо воно вже існує),
# створюємо нове правило брандмауера, яке блокує порт 3389 (порт RDP) для зазначеної IP-адреси,
# та записуємо інформацію про блокування в лог-файл.
#
foreach ($ip in $getip)
{
    $ruleName = "BlockRDPBruteForce_" + $ip.Name.Replace('.', '_')
    # Перевірка наявності правила. Якщо існує, то видаляємо
    if (Get-NetFirewallRule -DisplayName $ruleName -ErrorAction SilentlyContinue) {
        Remove-NetFirewallRule -DisplayName $ruleName
    }
    # Створюємо нове правило брандмауера для поточної IP-адреси
    Write-Output "Заблокована IP-адреса:" $ip.Name
    New-NetFirewallRule -DisplayName $ruleName -RemoteAddress $ip.Name -Direction Inbound -Protocol TCP -LocalPort 3389 -Action Block
    $blockedAttempts = ($badRDPlogons | Where-Object {$_.IpAddress -eq $ip.Name}).Count
    $logEntry = (Get-Date).ToString() + ' ' + $ip.Name + ' IP заблокована за ' + $blockedAttempts + ' спроб за 10 хвилин'
    $logEntry >> $log  # Запис події блокування IP-адреси в лог-файл
}

```

Рисунок 3.1 – Сценарій PowerShell для блокування IP зловмисника

Збережемо цей сценарій в теці C:\Bruteforce з назвою blockIPbruteforceRDPServer.ps1

У цьому скрипті PowerShell використовується для аналізу журналу подій "Security" і знаходження спроб підбору паролів через RDP. Давайте розглянемо, як відбувається цей процес:

1) Змінна `$LogName` визначає назву журналу подій, який ми хочемо аналізувати. У цьому випадку, ми використовуємо журнал подій "Security", оскільки саме він містить інформацію про автентифікацію та безпеку;
2) Функція `Get-WinEvent` використовується для отримання подій з журналу подій, використовуючи задані фільтри. У нашому випадку, ми використовуємо фільтри, що включають час початку аналізу, ID події

(4625 - невдалий вхід на систему) та тип входу (RDP). Результат отримується у змінну `$badRDPlogons`;

3) За допомогою функції `Where-Object` ми фільтруємо події зі змінної `$badRDPlogons`, застосовуючи додаткові умови. У цьому випадку, ми перевіряємо, що повідомлення події містить ключову фразу "`logon type: 3`", що вказує на вхід через RDP;
4) За допомогою функції `Select-Object` ми вибираємо потрібні властивості зі співставленнями. У нашому випадку, ми вибираємо IP-адреси з подій і присвоюємо їх властивості `IpAddress`;
5) Далі, за допомогою функції `Group-Object` ми групуємо IP-адреси зі змінної `$badRDPlogons` і обчислюємо кількість спроб для кожної IP-адреси. Функція `Where-Object` дозволяє відфільтрувати лише ті IP-адреси, які мають більше 5 спроб;
6) Знайдені IP-адреси зберігаються у змінній `$getip`;
7) Далі ми використовуємо цикл `foreach` для обробки кожної IP-адреси зі змінної `$getip`. Для кожної IP-адреси ми генеруємо унікальну назву правила брандмауера, перевіряємо, чи існує вже таке правило, та його видаляємо. Потім створюємо нове правило брандмауера, що блокує вказану IP-адресу на порті 3389 (RDP);
8) Ми також обчислюємо кількість спроб підбору паролів для кожної IP-адреси, використовуючи функцію `Where-Object`. Після цього ми формуємо повідомлення про блокування IP-адреси, яке включає дату, IP-адресу та кількість спроб;
9) Інформація про блокування IP-адреси записується в лог-файл, використовуючи оператор >>.

Подія 4625, яку ми використали для сценарію, відноситься до системи журналювання подій Windows, а саме до коду події "Audit Failure" (Помилка аудиту). Цей код події вказує на невдалі спроби аутентифікації або входи в систему.

Ця подія може виникати при різних методах входу в Windows Server. Не тільки через віддалений робочий стіл. Подія 4625 також може виникати при

невдалих спробах аутентифікації через мережеві протоколи, такі як SMB, FTP або інші протоколи, що дозволяють доступ до файлів та ресурсів на сервері.

В загальному, подія 4625 "Audit Failure" може виникати при будь-яких спробах аутентифікації або входу в Windows Server, які призводять до невдалого результату. Це можуть бути спроби локального входу, входу через віддалений робочий стіл або використання мережевих протоколів для доступу до сервера.

На рисунку 3.2 показано приклад такої події при виконанні brute-force атаки.

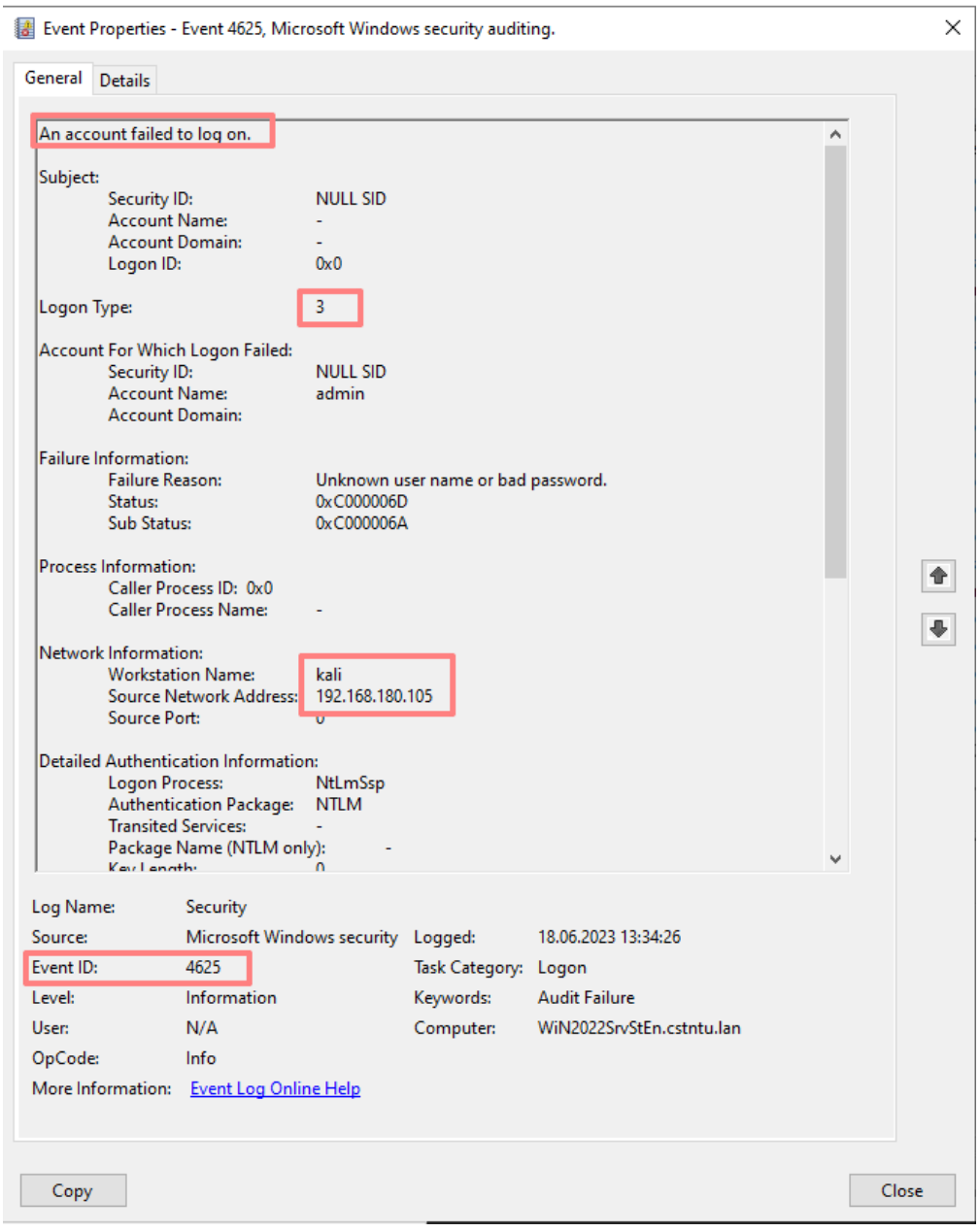

Рисунок 3.2 – Приклад події 4625 в журналі подій

Отже, скрипт PowerShell дозволяє аналізувати журнали подій системи, знаходити спроби підбору паролів через RDP та блокувати відповідні IP-адреси в брандмауері Windows.

3.1.3 Автоматизація процесу блокування IP

Для автоматичного запуску сценарію PowerShell при виникненні в журналі поді Windows Server події 4625, яка вказує на спроби атаки brute-force використаємо планувальник завдань (Task Scheduler) [11].

Task Scheduler є інструментом у Windows, який дозволяє автоматизувати виконання різних завдань на комп'ютері або сервері за заданим графіком або у відповідь на певні події. Цей інструмент дозволяє створювати завдання, які будуть виконуватися автоматично без необхідності постійного контролю або втручання користувача. Task Scheduler може виконувати різні типи завдань, такі як запуск програм або сценаріїв, виконання командних рядків, запуск скриптів PowerShell, встановлення або виконання системних операцій, відправлення повідомлень і багато іншого. Такі завдання можуть бути заплановані на виконання один раз або періодично за заданим розкладом.

Планувальник завдань також може бути налаштований на виконання завдань у відповідь на певні події або умови. Наприклад, ви можете створити завдання, яке автоматично запускається при запуску системи або після певного часу простою системи. Ви також можете налаштувати завдання, яке починається після виникнення певної події, наприклад, завантаження певного програмного забезпечення або входу користувача. За допомогою Task Scheduler можна автоматизувати різні завдання, які спрощують адміністрування та підтримку системи. Наприклад, можна налаштувати завдання резервного копіювання даних, очищення тимчасових файлів, оновлення програмного забезпечення або виконання скриптів для моніторингу та обслуговування системи.

Планувальник завдань в Windows дозволяє створювати розклади для виконання певних дій на основі певних тригерів, включаючи події системи.

На рисунках 3.3-3.5 показано приклад такого налаштування.

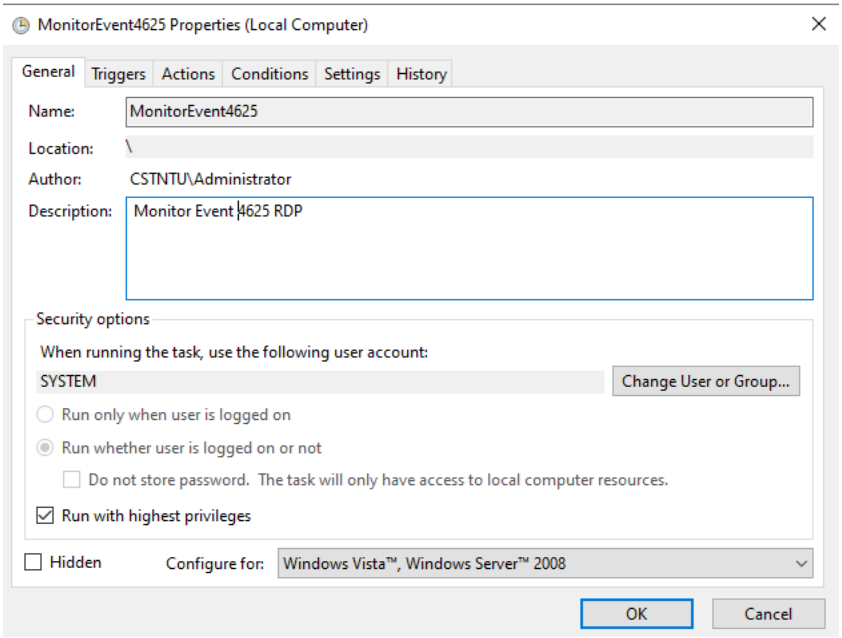

Рисунок 3.3 – Загальні налаштування події

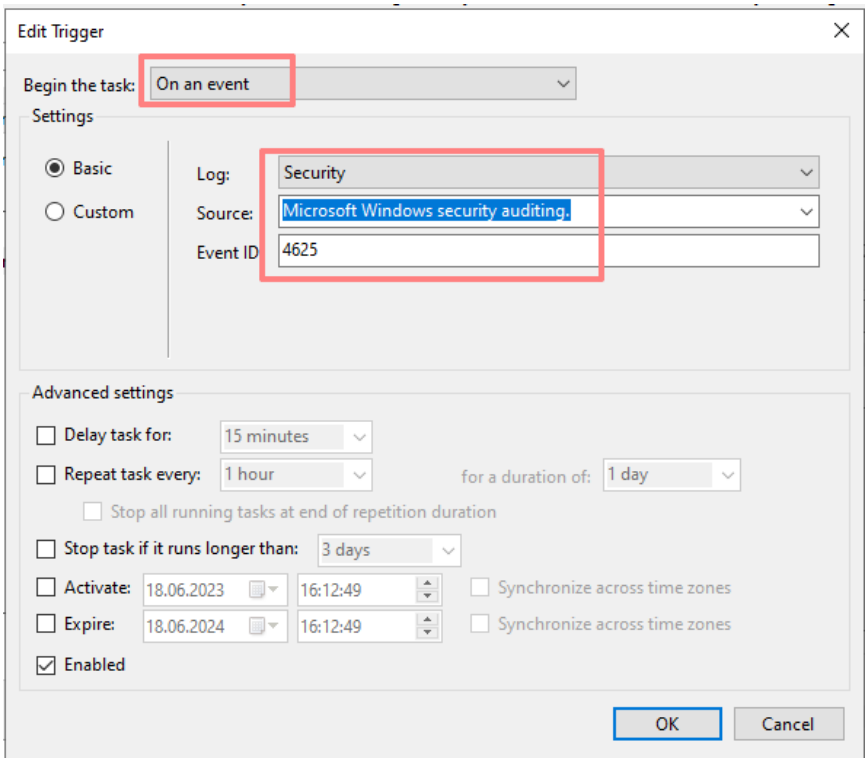

Рисунок 3.4 – Налаштування умови (trigger) для запуску події

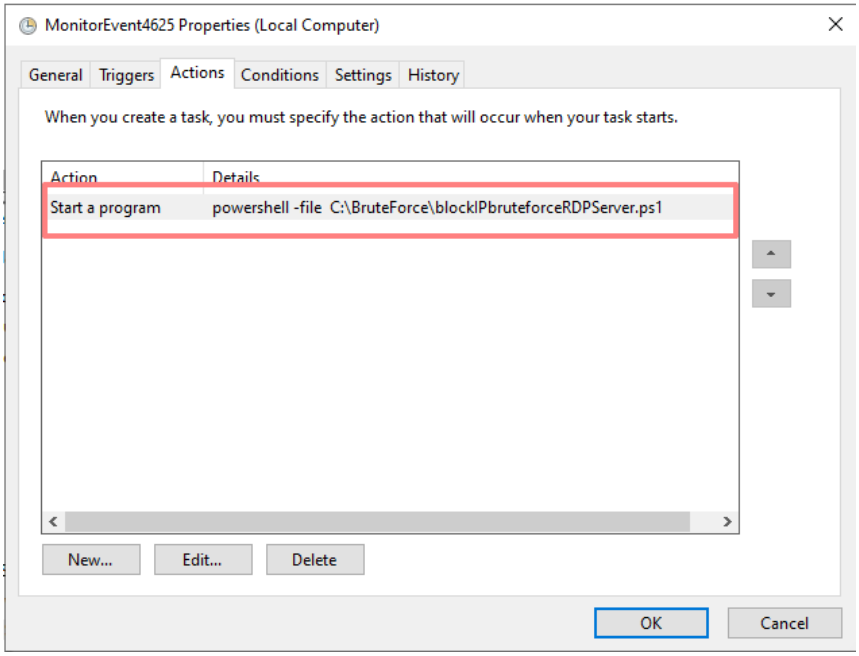

Рисунок 3.5 – Вказання шляху до PowerShell сценарію

Цей приклад показує, як можна автоматизувати блокування IP-адрес з надлишковими невдалими спробами авторизації через RDP.

Після цих кроків планувальник завдань буде моніторити події з журналу подій безпеки і автоматично запускати сценарій PowerShell, коли виявиться атака brute-force (події 4625).

3.2 Тестування системи автоматичного блокування IP зловмисника

Для тестування працездатності розробленого та налаштованого механізму блокування IP зловмисників при brute-force атаці проведемо тестову атаку ідентичну як в пункті 2.4.

Встановимо для порогу блокування облікового запису користувача значення 25. Даний поріг блокування не повинен спрацьовувати. Він буде лише як додатковий засіб безпеки. IP зловмисника має бути заблоковане до досягнення порогу блокування.

На рисунку 3.6 можна побачити що підбір паролю користувача пройшов невдало навіть попри те що ми навмисно явно вказали ім’я користувача Admin в параметрах запуску Hydra.

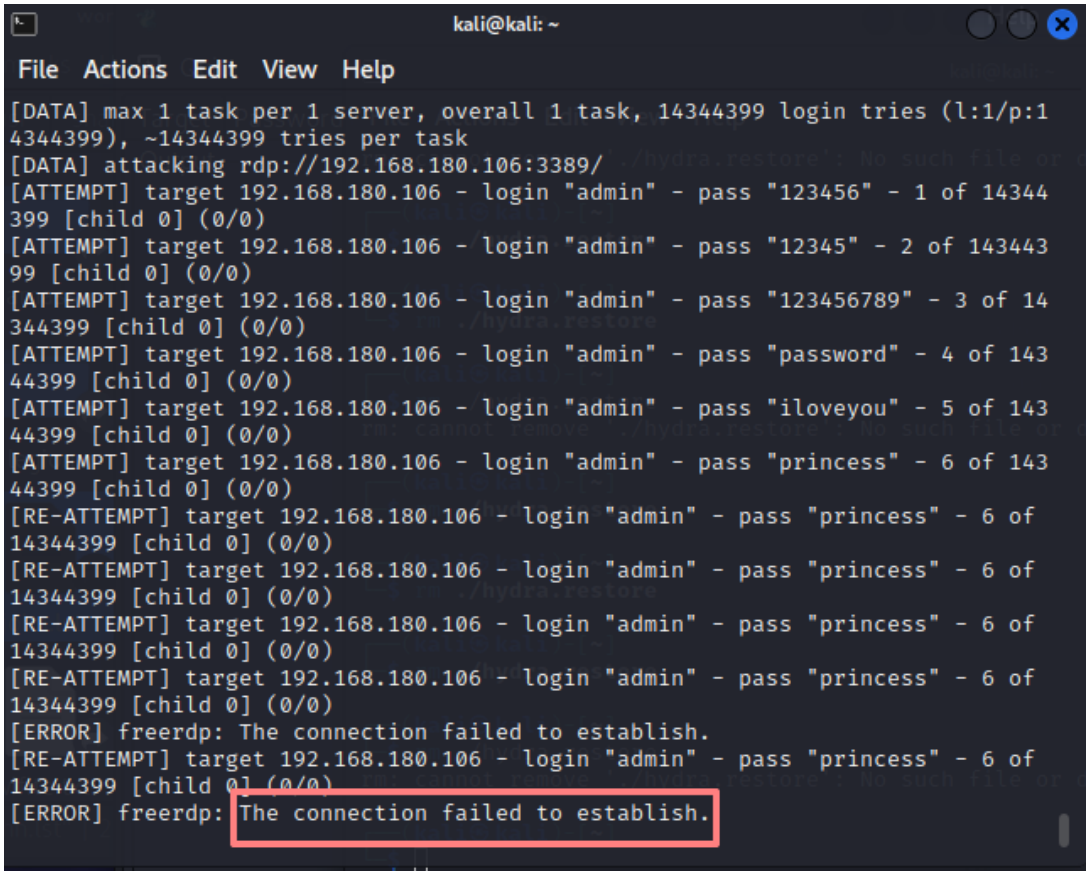

Рисунок 3.6 – Невдала спроба brute-force атаки при застосуванні сценарію блокування IP

Як видно з рисунку 3.6 відбулось блокування з'єднання з RDP сервером. Це підтверджується повідомлення `The connection failed to establish` та створеним новим правило брандмауера в Windows Server, яке блокує порт 3389 (порт RDP) для IP-адреси Kali Linux (Рис.3.7).

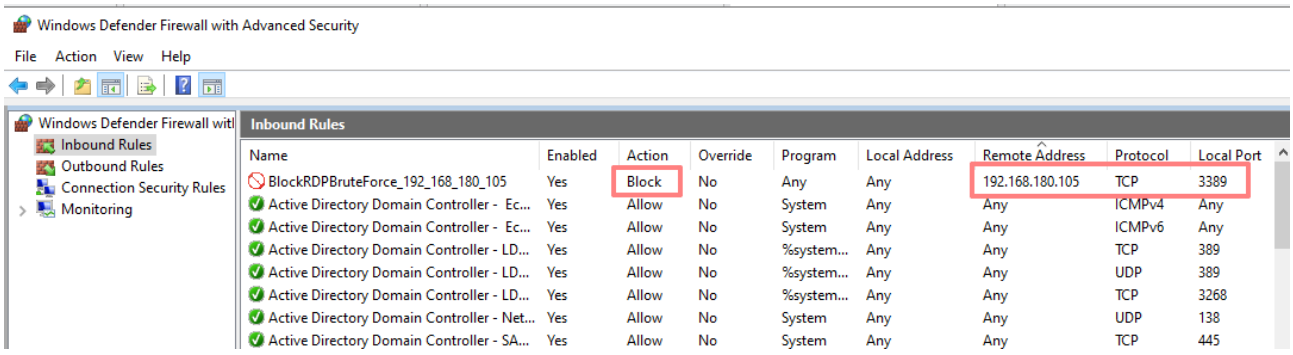

Рисунок 3.7 – Правило брандмауера в Windows Server, яке блокує порт 3389 та IP 192.168.180.105

Також лог-файл C:\Bruteforce\blocked_bruteforce_ip.txt в який сценарій PowerShell здійснює запис події блокування IP-адреси містить заблоковану IP 192.168.180.105 (Рис.3.8).

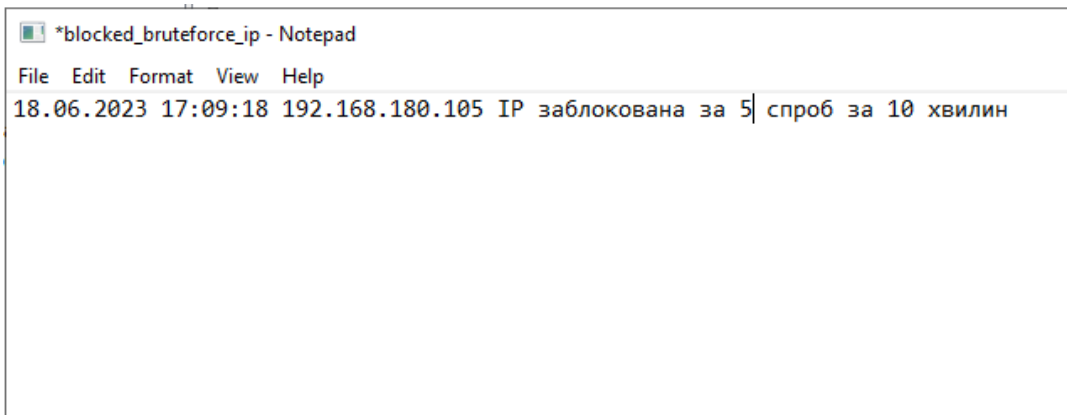

Рисунок 3.8 – Вміст файлу blocked_bruteforce_ip.txt

Цей результат підтверджує, що скрипт PowerShell виконав свою функцію і автоматично додав правило брандмауера, яке блокує доступ до RDP порту для IP-адреси Kali Linux. Це є ефективним заходом для захисту від brute-force атак, оскільки з'єднання з RDP сервером заблоковане для IP-адреси зловмисника.

Для переконання в правильності блокування встановимо з'єднання з іншого пристрою (Ubuntu Linux з IP адресом 192.168.180.103), який має дозвіл на доступ до RDP сервера (Рис.3.9).

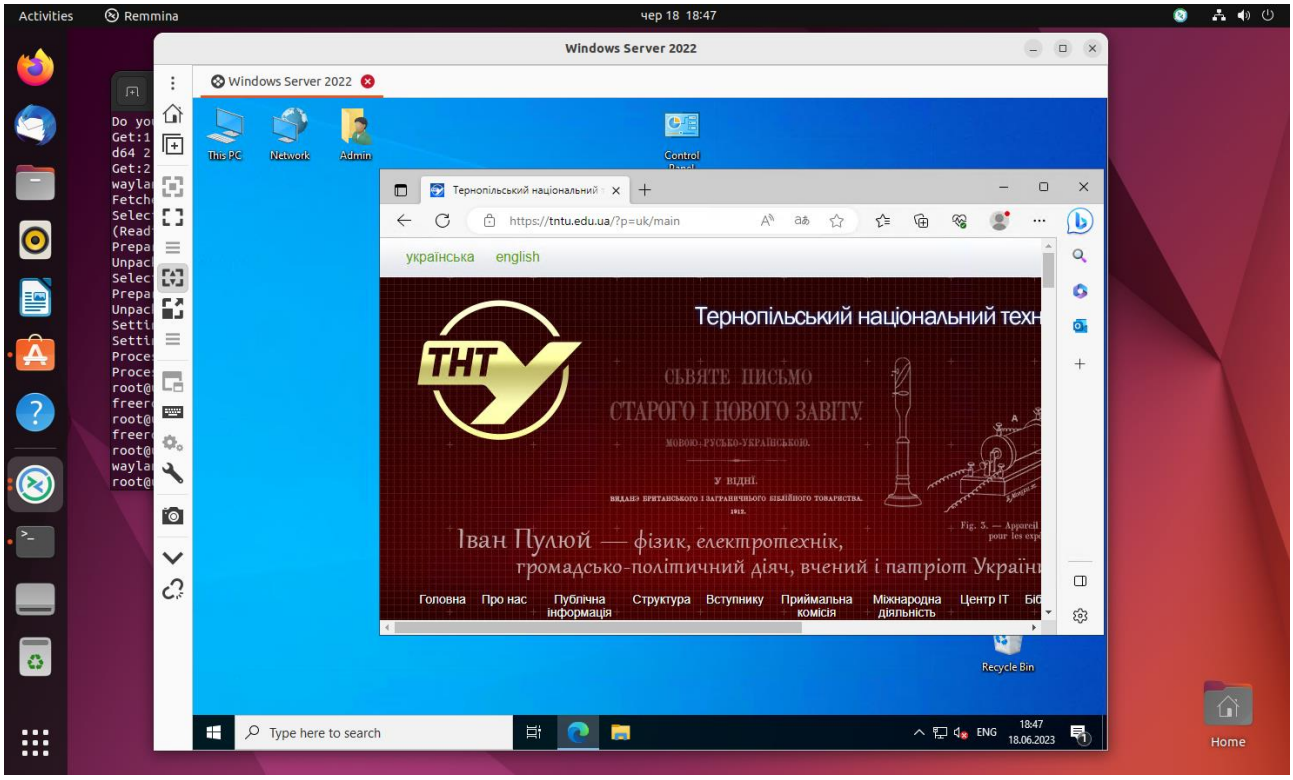

Рисунок 3.9 – Перевірка доступу до Windows Server по RDP з IP 192.168.180.103

Блокування IP-адреси та складні паролі є досить надійним методом захисту від brute-force атак на Windows Server через RDP.

Розроблена система автоматичного блокування IP-адреси зловмисника на основі події 4625 може бути успішно використана не лише для виявлення і блокування brute-force атак через RDP, але й для інших варіантів brute-force атак в операційній системі Windows Server.

Подія 4625 є загальною подією аудиту безпеки, яка реєструє невдалий процес аутентифікації або входу в систему. Такі невдалі спроби можуть відбуватися в різних ситуаціях, включаючи несанкціонований доступ до системи через різні протоколи, служби або мережеві ресурси.

Розроблена система, аналізуючи подію 4625 і виявляючи невдалий процес аутентифікації, може виконувати автоматичне блокування IP-адреси зловмисника, незалежно від того, який протокол або механізм аутентифікації був використаний для атаки. Це дозволяє ефективно захищати операційну систему від різних варіантів brute-force атак, які можуть спрямовуватися на різні складові системи або послуги.

Таким чином, розроблений модуль є універсальним і може бути застосований для виявлення та блокування brute-force атак у різних сценаріях в операційній системі Windows Server. Він дозволяє підвищити безпеку системи, незалежно від того, який конкретний метод атаки був використаний зловмисником.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Вимоги пожежної безпеки при гасінні електроустановок

Електроустановки є потенційно небезпечними місцями для виникнення пожеж, так як вони містять велику кількість горючих матеріалів і речовин (ізоляційні матеріали, масла) і потенційні джерела займання (коротке замикання, скачки напруги, перевантаження, іскри). Таке поєднання пожежонебезпечних факторів призводить до того, що саме суворе дотримання норм безпеки не може повністю усунути можливість виникнення пожежі.

Основними причинами виникнення вогнищ горіння або задимлення в електроустановках є:

- аварійні ситуації, пов'язані з перевантаженням в електромережі при відсутності захисту необхідного рівня;
- коротке замикання через пошкодження обладнання або ліній електропередач;
- несправності технологічного обладнання;
- ушкодження допоміжних електромереж;
- порушення правил експлуатації і людський фактор.

Додатковим фактором небезпеки під час пожежі в електроустановках є висока напруга - найчастіше аварійні умови не дозволяють зняти напругу на охопленому вогнем ділянці, тим більше що ситуація вимагає екстрених заходів і швидких рішень. Саме тому кожному співробітнику, задіяному в роботі на такому обладнанні, необхідно точно знати - як і чим слід гасити вогнище загоряння в електроустановках до 1000 В.

Промислові електроустановки в більшості випадків мають автоматичні засоби пожежогасіння, які починають роботу при перевищенні заданих температурних параметрів в приміщенні, аварійному відключенні електроживлення обладнання та інших факторах. При відсутності такої системи виник осередок займання або задимлення необхідно ліквідувати своїми засобами і силами до приїзду фахівців Державної служби з надзвичайних ситуацій України.

Правила пожежної безпеки України регламентують використання первинних засобів пожежогасіння на електроустановках. Згідно цих правил для гасіння електроустановок які не знаходяться під напругою можна використовувати пісок, воду і вогнегасники всіх марок. Якщо електроустановка перебуває під напругою до 1000 В - дозволено використовувати для придушення осередків займання або задимлення тільки вогнегасники порошкового, аерозольного або вуглекислотного типів з дотриманням всіх правил безпеки [12].

При виникненні вогнища загоряння в щитах управління під напругою до 400В допускається використання вуглекислотних, аерозольних або порошкових типів вогнегасників. Якщо вогнище придушити не вдається, то допускається використання розпорошених водяних потоків від протипожежного водопроводу або спеціальної техніки з обов'язковим дотриманням правил безпеки - із застосуванням електроізолюючих рукавичок, взуття, індивідуальні засоби захисту, із заземленням пожежного ствола і насоса спецтехніки.

Під час гасіння пожежі електроустановок під напругою забороняється [13]:

- використання усіх видів піни;
- проводити будь-які відключення та інші операції з електричним обладнанням особовому складу пожежних підрозділів;
- використовувати воду зі змочувачами при подаванні компактних струменів води, як для гасіння, так і для охолодження електрообладнання та будівельних конструкцій;
- наближатися до машин і механізмів, які застосовуються для подачі води (вогнегасних речовин) на електроустановки під напругою, особам, безпосередньо не зайнятим на гасінні пожежі.

Ефективно застосовується вогнегасник, коли правильно вибрано його тип враховуючи клас пожежі, яку потрібно гасити. Вогнегасники, які містять вуглекислий газ, працюють на основі низькотемпературного струменя і відносяться до газового потоку. Після використання такого вогнегасника не залишається ніяких слідів. Однак, не слід використовувати вуглекислотні вогнегасники в замкнутому просторі, так як існує ризик пошкодження шкіри і отруєння.

Гасіння електроустановок під напругою за допомогою порошкового вогнегасника вважається ефективним методом усунення загоряння. Порошок, присутній в складі, запобігає доступ кисню до матеріалу і, отже, перешкоджає поширенню полум'я, усуваючи повторні спроби загоряння.

В інструкції до вогнегасника обов’язково міститься інформація про дату виготовлення та час проведення його останнього техобслуговування.

4.2 Техніка безпеки при роботі з ПК

До самостійної роботи на комп’ютерах допускаються особи, які пройшли медичний огляд, навчання по професії, вступний інструктаж з охорони праці та первинний інструктаж з охорони праці на робочому місці. В подальшому вони проходять повторні інструктажі з охорони праці на робочому місці один раз на півріччя, періодичні медичні огляди один раз на два роки.

Під час роботи на комп’ютерах можуть діяти такі небезпечні та шкідливі фактори, як:

- фізичні;
- психофізіологічні.

Основним обладнанням робочого місця користувача комп’ютера є монітор, системний блок та клавіатура, мишка.

Робочі місця мають бути розташовані на відстані не менше 1,5 м від стіни з вікнами, від інших стін на відстані 1м, між собою на відстані не менше 1,5 м. Відносно вікон робоче місце доцільно розташовувати таким чином, щоб природне світло падало на нього збоку, переважно зліва.

Робочі місця слід розташовувати так, щоб уникнути попадання в очі прямого світла. Джерела освітлення рекомендується розташовувати з обох боків екрану паралельно напрямку погляду. Для уникнення світлових відблисків екрану, клавіатури в напрямку очей користувача, від світильників загального освітлення або сонячних променів, необхідно використовувати анти полискові сітки, спеціальні фільтри для екранів, захисні козирки, на вікнах – жалюзі.

Монітор повинен бути розташований на робочому місці так, щоб поверхня екрана знаходилася в центрі поля зору на відстані 400-700 мм від очей користувача. Рекомендується розміщувати елементи робочого місця так, щоб витримувалася однакова відстань очей від екрана, клавіатури, тексту.

Зручна робоча поза при роботі з комп'ютером забезпечується регулюванням висоти робочого столу, крісла та підставки для ніг. Раціональною робочою позою може вважатися таке положення, при якому ступні працівника розташовані горизонтально на підлозі або підставці для ніг, стегна зорієнтовані у горизонтальній площині, верхні частини рук – вертикальні. Кут ліктєвого суглоба коливається в межах 70-90°, зап'ястя зігнуті під кутом не більше ніж 20°, нахил голови 15-20°.

Для нейтралізації зарядів статичної електрики в приміщенні, де виконується робота на комп'ютерах, в тому числі на лазерних та світлодіодних принтерах, рекомендується збільшувати вологість повітря за допомогою кімнатних зволожувачів. Не рекомендується носити одяг з синтетичних матеріалів.

Згідно статті 18 Закону України "Про охорону праці" працівник зобов'язаний:

- знати і виконувати вимоги нормативних актів про охорону праці, правила поводження з устаткуванням та іншими засобами виробництва, користуватися засобами колективного та індивідуального захисту;
- дотримуватись зобов'язань щодо охорони праці, передбачених колективним договором та правилами внутрішнього трудового розпорядку підприємства;
- співробітничати з власником у справі організації безпечних і нешкідливих умов праці, особисто вживати посильних заходів щодо усунення будь-якої виробничої ситуації, яка створює загрозу його життю чи здоров'ю, або людей, які його оточують, повідомляти про небезпеку свого безпосереднього керівника або іншу посадову особу.

Вимоги безпеки перед початком роботи:

- увімкнути систему кондиціювання в приміщенні;

- перевірити надійність встановлення апаратури на робочому столі. Повернути монітор так, щоб було зручно дивитися на екран – під прямим кутом (а не збоку) і трохи зверху вниз, при цьому екран має бути трохи нахиленим, нижній його край ближче до оператора;
- перевірити загальний стан апаратури, перевірити справність електропроводки, з'єднувальних шнурів, штепсельних вилок, розеток, заземлення захисного екрана;
- відрегулювати освітленість робочого місця;
- відрегулювати та зафіксувати висоту крісла, зручний для користувача нахил його спинки;
- приєднати до системного блоку необхідну апаратуру. Усі кабелі, що з'єднують системний блок з іншими пристроями, слід вставляти та виймати при вимкненому комп'ютері;
- ввімкнути апаратуру комп'ютера вимикачами на корпусах в послідовності: монітор, системний блок, принтер (якщо передбачається друкування);
- відрегулювати яскравість свічення монітора, мінімальний розмір світної точки, фокусування, контрастність. Не слід робити зображення надто яскравим, щоб не втомлювати очей.

Рекомендується:

- яскравість свічення екрана – не менше 100Kg/м2;
- відношення яскравості монітора до яскравості оточуючих його поверхонь в робочій зоні – не більше 3:1;
- мінімальний розмір точки свічення не більше 0,4 мм для монохромного монітора і не менше 0,6 мм для кольорового, контрастність зображення знаку – не менше 0,8.

При виявленні будь-яких несправностей роботу не розпочинати, повідомити про це керівника.

Вимоги безпеки під час виконання роботи:

- необхідно стійко розташовувати клавіатуру на робочому столі, не опускати її хитання. Під час роботи на клавіатурі сидіти прямо, не напружуватися;
- для забезпечення несприятливого впливу на користувача пристроїв типу “миша” належить забезпечувати вільну велику поверхню столу для переміщення “миші” і зручного упору ліктьового суглоба;
- не дозволяються сторонні розмови, подразнюючі шуми;
- періодично при вимкненому комп’ютері прибирати ледь змоченою мильним розчином бавовняною ганчіркою порох з поверхонь апаратури. Екран протирають ганчіркою, змоченою у спирті. Не дозволяється використовувати рідинні або аерозольні засоби чищення поверхонь комп’ютера.

Психофізіологічне розвантаження є одним з варіантів зменшення стресу.

Дана практика включає в себе застосування методу аутогенного тренування, що передбачає свідоме використання комплексу прийомів психічної саморегуляції та виконання простих фізичних вправ зі словесним самонавіюванням. Основна увага приділяється розслабленню м'язів (релаксації).

Під час сеансів психофізіологічного розвантаження рекомендується використовувати три періоди, що відповідають фазам відновлення:

Перший період - абстрагування від виробничого середовища, що відповідає фазі залишкового збудження. В цей час відтворюється повільна мелодійна музика та звуки пташиного співу. Працівники знаходять зручну позу та психологічно готуються до наступних періодів.

Другий період - заспокоєння, що відповідає фазі відновлювального гальмування. Показуються фотослайди з зображеннями природи, таких як квітучі луки, березові гаї, ставки і т.д. Звуковий супровід включає спокійну музику та заспокійливі формули аутогенного тренування.

Третій період - активізація, що відповідає фазі підвищеної збудженості. Спочатку світло повністю вимикається, а потім на екрані появляється червона пляма, розмір і яскравість якої поступово збільшуються. В кінці періоду звучить

бадьора музика, а працівники виконують мобілізуючі формули аутогенного тренування, попередньо зробивши глибоке вдихання та видихання.

Сеанси психофізіологічного розвантаження можуть проводитись за єдиною програмою через індивідуальні навушники і складатись із двох періодів по 5 хвилин кожний: повне розслаблення та активізація працездатності. При необхідності, на фоні музики можуть використовуватись фрази, що сприяють відпочинку, покращенню самопочуття та бадьорості на заключному етапі. Після сеансів психофізіологічного розвантаження працівники відчувають зменшення втоми, з'являється бадьорість та гарний настрій, а загальний стан помітно поліпшується.

Додатково до сеансів психофізіологічного розвантаження, працівники також можуть скористатись іншими методами для зниження стресу та покращення психологічного благополуччя.

Одним з ефективних підходів є впровадження регулярних перерв під час робочого дня. Це можуть бути короткі паузи, під час яких працівники займаються розслаблюючими вправами, дихальними техніками або просто відпочивають. Це допомагає знизити напругу і покращити фокусування під час робочого процесу.

Також важливо створити комфортне робоче середовище для працівників. Це може включати забезпечення комфортних стільців і столів, добре освітлення та достатню вентиляцію. Природне освітлення та наявність рослин у приміщенні також можуть позитивно вплинути на настрій та самопочуття працівників.

Підтримка від керівництва та колег також має важливе значення. Створення сприятливого та підтримуючого робочого середовища, де працівники можуть відчути підтримку та співпрацю, сприяє зниженню стресу та покращує загальний настрій в колективі.

Крім того, особисте самоуправління і здібність до саморегуляції є важливими навичками для працівників. Це включає уміння регулювати власні емоції, реагувати на стресові ситуації та знаходити способи їх подолання, наприклад, за допомогою медитації, йоги або інших релаксаційних технік.

Усі ці підходи сприяють створенню здорової та продуктивної робочої атмосфери, де працівники можуть ефективно керувати стресом, забезпечуючи своє фізичне та емоційне благополуччя.

ВИСНОВКИ

У ході кваліфікаційної роботи було проведено дослідження проблеми brute-force атак на операційну систему Windows Server 2022 та розроблено ефективні методи захисту від таких атак. Brute-force атаки є поширеним методом злому систем, що може призвести до несанкціонованого доступу до даних та порушення безпеки інформаційної інфраструктури організацій.

У рамках роботи було розглянуто різні механізми та заходи безпеки, які можуть бути використані для захисту від brute-force атак. Були запропоновані механізми політики паролів, блокування пароля після невдалих спроб входу та фільтрації трафіку через брандмауер.

Для ефективного виявлення та блокування brute-force атак була розроблена система на базі PowerShell, яка аналізує журнал подій на Windows Server та автоматично блокує IP-адреси зловмисників за допомогою Windows Firewall. Постійний моніторинг наявності атаки забезпечується за допомогою планувальника завдань, який виконує сценарій при заданих умовах.

Важливість розробленої системи полягає в її універсальності та широкому спектрі застосування. Вона може успішно застосовуватися для виявлення та блокування brute-force атак не лише через RDP, але й у будь-яких інших варіантах атак, що спрямовані на операційну систему Windows Server.

Результати даної роботи дозволять підвищити рівень захисту операційної системи Windows Server 2022 від brute-force атак та забезпечити надійність та безпеку інформаційних ресурсів організацій. Розроблені методи та сценарії можуть бути використані адміністраторами систем для покращення захисту серверів та запобігання несанкціонованому доступу до системи.

Також дана кваліфікаційна робота може бути використана в навчальних цілях. Розроблені методи та сценарії можуть слугувати прикладами і практичними вправами для студентів, які вивчають безпеку операційних систем та мереж.

Студенти зможуть ознайомитися з концепцією brute-force атак, їх наслідками та вивчити методи захисту від таких атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Brute Force Attack [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. –Режим доступу: https://www.imperva.com/learn/application-security/brute-force-attack/
2. How to Prevent Brute Force Attacks [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – Режим доступу: https://www.itsasap.com/blog/how-to-prevent-brute-force-attacks
3. Technical documentation [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – Режим доступу: https://learn.microsoft.com/en-us/docs/
4. Remote Desktop Services [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – Режим доступу: https://learn.microsoft.com/en-us/windows/win32/termserv/terminal-services-portal
5. RDP brute force attacks explained [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – https://www.malwarebytes.com/blog/news/2021/08/rdp-brute-force-attacks-explained
6. Password Policy [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – Режим доступу: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy
7. Account Lockout Policy [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – Режим доступу: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-policy
8. Kali Linux Official Documentation [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – Режим доступу: https://www.kali.org/docs/
9. Kali Linux Tool Documentation: hydra [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – Режим доступу: https://www.kali.org/tools/hydra/

10. PowerShel [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – Режим доступу: https://learn.microsoft.com/uk-ua/windows-server/administration/windows-commands/powershell
11. How to schedule a server process [Електронний ресурс] : [Інтернет-портал]. – Електронні дані. – Режим доступу: https://learn.microsoft.com/en-us/troubleshoot/windows-server/system-management-components/schedule-server-process
12. Міністерство енергетики та вугільної промисловості України. Наказ, Інструкція Про затвердження Інструкції з гасіння пожеж на енергетичних об'єктах України // Відомості Верховної Ради України (ВВР). 2011. URL: https://zakon.rada.gov.ua/laws/show/z0013-12 (дата звернення: 15.05.2021).
13. Костюк В. Гасіння пожеж на електричних об'єктах під напругою // Охорона праці і пожежна безпека. 2018.