Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Залевського Максима Владиславовича*

академічної групи *125-18-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Підсистема захисту інформації робочої станції оператора коллцентра банківської установи*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц Герасіна О.В.			
розділів:				
спеціальний	ас. Мілінчук Ю.А.			
економічний	к.е.н., доц. Пілова Д.П.	85	Добре	

Рецензент				

Нормоконтролер	ст. вик. Тимофєєв Д. С.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____2022року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Залевському М.В.* **академічної групи** *125-18-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Підсистема захисту інформації робочої станції оператора коллцентра банківської установи*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 18.05.2022 № 268-с

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Постановка задачі. Визначення актуальності питання. Аналіз ІТС у якої знаходиться робоча станція. Аналіз усунених загроз.	06.05.2022
Розділ 2	Усунення вразливостей робочої станції	19.05.2022
Розділ 3	Розрахунок економічних показників запропонованих рішень	02.06.2022

Завдання видано _____ Герасіна О.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 21.01.2022

Дата подання до екзаменаційної комісії: 9.06.2022

Прийнято до виконання _____ Залевський М.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 58с., 14 рис., 1 табл., 2 додатка, 14 джерел.

Об'єкт розробки: ІТС колцентра банківської установи.

Предмет розробки: захист робочої станції колцентру банківської установи від загроз витоку інформації.

Мета роботи: розробка підсистеми захисту інформації робочої станції колцентра банківської установи.

У першій частині описано робоче місце оператора та мережу колцентра, вразливості що можуть привести до витоку інформації та наявні засоби захисту, проводиться вибір оптимальної ОС для робочого місця.

У спеціальній частині проаналізовано вразливості мережевих протоколів ОС, вразливості використання SAMBA серверу у мережі, загрози витоку інформації з робочої станції оператора колцентра та запропоновано методи щодо їх усунення.

В економічному розділі визначено економічну ефективність впровадження запропонованих методів щодо усунення загроз витоку інформації з робочої станції оператора колцентра.

Практичне значення роботи полягає в розробці рекомендацій щодо створення підсистеми захисту робочої станції колцентра банківської установи.

Результати роботи можуть бути використані для поліпшення безпеки інформації будь-яких установ, використовуючих ОС Windows.

КЛЮЧОВІ СЛОВА: ВИТОК ІНФОРМАЦІЇ, ОПЕРАЦІЙНА СИСТЕМА WINDOWS, МЕРЕЖЕВІ ПРОТОКОЛИ, ACTIVE DIRECTORY, ВРАЗЛИВОСТІ ЗІ СТОРОНИ КОРИСТУВАЧА, SMB, LLMNR, NBT-NS.

ABSTRACT

Explanatory note: 58 pages, 14 figures, 1 table, 2 appendices, 14 sources.

Object of research: information and telecommunication system of the call center of the banking institution

Subject of development: protection of the workstation of the call center of the banking institution from threats of information leakage.

Objective: development of recommendations for the creation of the iformational security subsystem for working station of the call center of the banking institution.

The first part describes the operator's workplace, the network in which the workstation is located, already existing measures of workstations information leakage prevententage, the relevance of vulnerabilities, demonstration of one of the methods of attack using these vulnerabilities, reviewed the possibility of switching to another operating system

The special part analyzes the possible threats of information leakage from the workstation, describes the reasons why they are present, provides specific ways to eliminate them for the current configuration.

The economic section identifies the cost-effectiveness of implementing the proposed measures to address these vulnerabilities.

The practical significance of this work is to study the vulnerabilities of the most widespread operating system in the world.

The results can be used to improve the security of information of any institution using Windows OS.

KEY WORDS: INFORMATION LEAK, WINDOWS OPERATING SYSTEM, NETWORK PROTOCOLS, ACTIVE DIRECTORY, WORKSTATION VULNERABILITIES, SMB, LLMNR, NBT-NS,

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ПЗ – Програмне забезпечення

ОС – операційна система

AD – Active Directory

WSUS – Windows server update service

SMB - Server Message Block

LDAP - Lightweight Directory Access Protocol

DNS - Domain Name System

NBT-NS - NetBIOS Name Service

LLMNR - Link-Local Multicast Name Resolution

mDNS - multicast DNS

WPAD - Web Proxy Autodiscovery Protocol

RDP - Remote Desktop Protocol

WPD - Windows Portable Devices

GUID - Globally Unique Identifier або Universally Unique Identifier

VNC - Virtual Network Computing

ЗМІСТ

ВСТУП

У цифрову епоху усі важливі документи та персональна інформація все більше переходить у цифровий формат, та все більше до звичайних старих важливих документів як паспорт та ідентифікаційний код додається ще й чутлива персональна інформація у вигляді обліковий даних, фотографії та відеозаписів, втрата чи потрапляння у руки зловмисника котрих несе важкі наслідки для їх власника.

Кожного дня безліч користувачів персональних комп'ютерів потрапляє під атаки зі сторони кіберзлочинців. При цьому є рідкістю коли користувачі піклуються про безпеку своїх даних до моменту атаки. Це на жаль є також розповсюдженою практикою у компаніях, де як показала практика, не піклуються про безпечність робочих місць та відмовляються зробити вклад у інформаційну безпеку щоб не допустити великі фінансові та репутаційні втрати аж до того моменту як станеться атака та компанія ці втрати понесе.

Зважаючи на те, що на робочій станції оператора коллцентра банківської установи зберігаються та оброблюються як персональні дані клієнтів, так і персональні дані оператора у виді облікових записів, задача запобігання витоку інформації з робочої постає досить актуальною.

Об'єктом розробки є ІТС колцентра банківської установи

Предмет розробки: захист робочої станції колцентру банківської установи від загроз витоку інформації.

Мета роботи: розробка підсистеми захисту інформації робочої станції колцентра банківської установи.

Для вирішення поставленої задачі необхідно визначити вразливості зі сторони робочої станції, що можуть призвести до втрати інформації та запропонувати способи їх усунення.

Практичне значення полягає в використанні запропонованих рішень для будь-якої компанії, що використовує персональні комп'ютери у роботі, та звичайних користувачів персонального комп'ютера.

1 СТАН ПИТАННЯ ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Незважаючи на те що зараз важко знайти бізнес який не використовує цифрові технології та не зберігає на персональних комп'ютерах важливу інформацію, дуже частим є рішення просто ігнорувати можливі загрози інформаційної безпеки.

При цьому загроза кібератак з кожним днем тількі зростає, бо зловмисники постійно шукають та знаходять нові вразливості інформаційної безпеки, а користувачи персональних комп'ютерів продовжують ігнорувати небезпеку продовжуючи запускати шкідливе ПЗ та відключати вбудовані заходи інформаційної безпеки, не говорячи про застосування додаткових.

Цьому служить прикладом нещодавні великі атаки WannaCry [1] та NotPetya [2], яки призвели до величезних втрат та на деякий час повністю зупинили інформаційний сектор багатьох компаній.

Не усунені вразливості робочих станції можуть призвести не тільки до витоку персональних файлів та даних, а й в тому числі до витоку облікових даних користувача, що надає змогу зловмиснику отримати доступ до будь яких ресурсів де вони використовуються, а у разі робочої станції компанії – отримати доступ до внутрішнії ресурсів цієй установи де знаходяться конфіденційні дані та дані клієнтів цієй компанії, що призведе до дуже великих економічних та репутаційних втрат. Також облікові дані могуть надати змогу зловмиснику дистанційно під'єднуватися та керувати персональним комп'ютером без відома користувача чи змусити комп'ютер запускати будь-яке ПЗ зловмисника.

У роботі будуть розглянуті взразливості зі сторони робочої станції оператора колцентра банківської установи. У поточній конфігурації це вразливості присутні у ОС Windows.

Ці вразливості актуальні через те що вони присутні у любому персональному комп'ютері під керуванням ОС Windows, яка є найпопулярнішою у світі.

При цьому, як буде продемонстровано, реалізація атак через ци вразливості не вимагає від зловмисника майже ніяких технічних знань та навичків, та може виконуватися за допогою безкоштовного загальнодоступного ПЗ.

Тому необхідно проаналізувати та визначити способи ліквідації цих вразлиовстей для поточної конфігурації інформаційної системи установи та додатково проаналізувати можливість переходу на ОС Linux.

Згідно дослідженням [3], кожні 39 секунд відбувається кібер атака на персональний комп'ютер з доступом до глобальної мережі та кожні 44 секунди відбувається виток інформації, як персональних даних користувачів так й даних клієнтів які зберігаються на робочих станціях компаній. При цьому 95% випадків витоку інформації відбувається через дії користувача персонального комп'ютеру, що ще раз демонструє важливість забезпечення безпеки саме робочої станції, а не мережі в якій вона знаходиться.

Вважаючи на те що вразливості робочої станції будуть розглядатися з боку саме операційної системи та ПЗ, а операційна система яка використовується у даному випадку це Windows, це ще більше підвищує актуальність питання. Це пов'язано з тим що саме ОС Windows є самою розповсюдженою у світі. Але, як можна побачити на рисунку 1.1, використання саме цієї ОС складає 75% для персональних комп'ютерів у всьому світі (статистика наведена як для персонального використання, так і для бізнес сектору) що не просто займає першу позицію по популярності, а й у п'ять разів перевищує використання другої по розповсюдженості ОС. Наслідком цього є те що майже все шкідливе програмне забезпечення виробляється виключно для ОС Windows.

Тобто стає зрозуміло що знайдені вразливості є актуальними не тільки для робочих станції конкретно розглянутого коллцентра банківської установи, а й для 75% відсотків користувачів персональних комп'ютерів у всьому світі. Також для наочності буде продемонстровано наскільки легко провести атаку на персональний комп'ютер з ОС Windows.

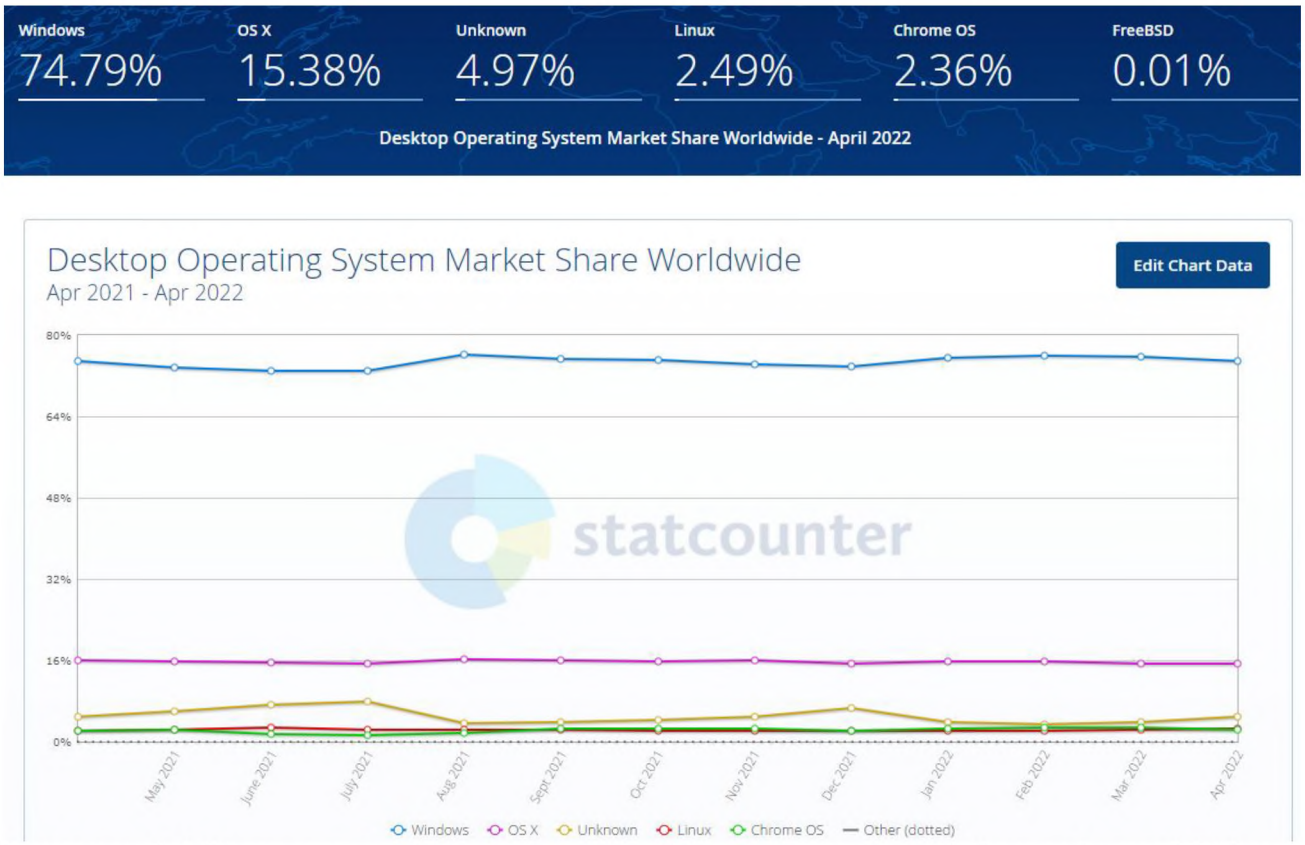


Рисунок 1.1 Частка використання операційних систем у світі на квітень 2022 року [4]

1.2 Вразливості ОС Windows

Для демонстрації атаки буде використовуватися Responder[5] - безкоштовне ПЗ з відкритим кодом, написане на програмному язику python. ПЗ є отруйником LLMNR, NBT-NS та MDNS запитів, тобто воно надсилає «отруєні» відповіді на запити інших машин у мережі змушуючи машину сприймати спеціально налаштовані фальшиви сервери цього ПЗ як легітимні, дозволяючи провести атаку типу чоловік по середині. Responder буде слухати та відповідати тільки на специфічні запити, через що виглядає у мережі як типовий персональний комп'ютер доки він не почне надсилати відповіді, та навіть під час того як він передає отруєні відповіді, він буде виглядати як звичайний файловий сервер, сервер аутентифікації чи сервер який зберігає конфігураційний файл проксі-серверу.

Буде використовуватися загальнодоступний безкоштовний дистрибутив з відкритим кодом Linux Kali [6] на базі Debian, який має багато попередньо інстальованого ПЗ для перевірки вразливостей [7], у тому числі і Responder.

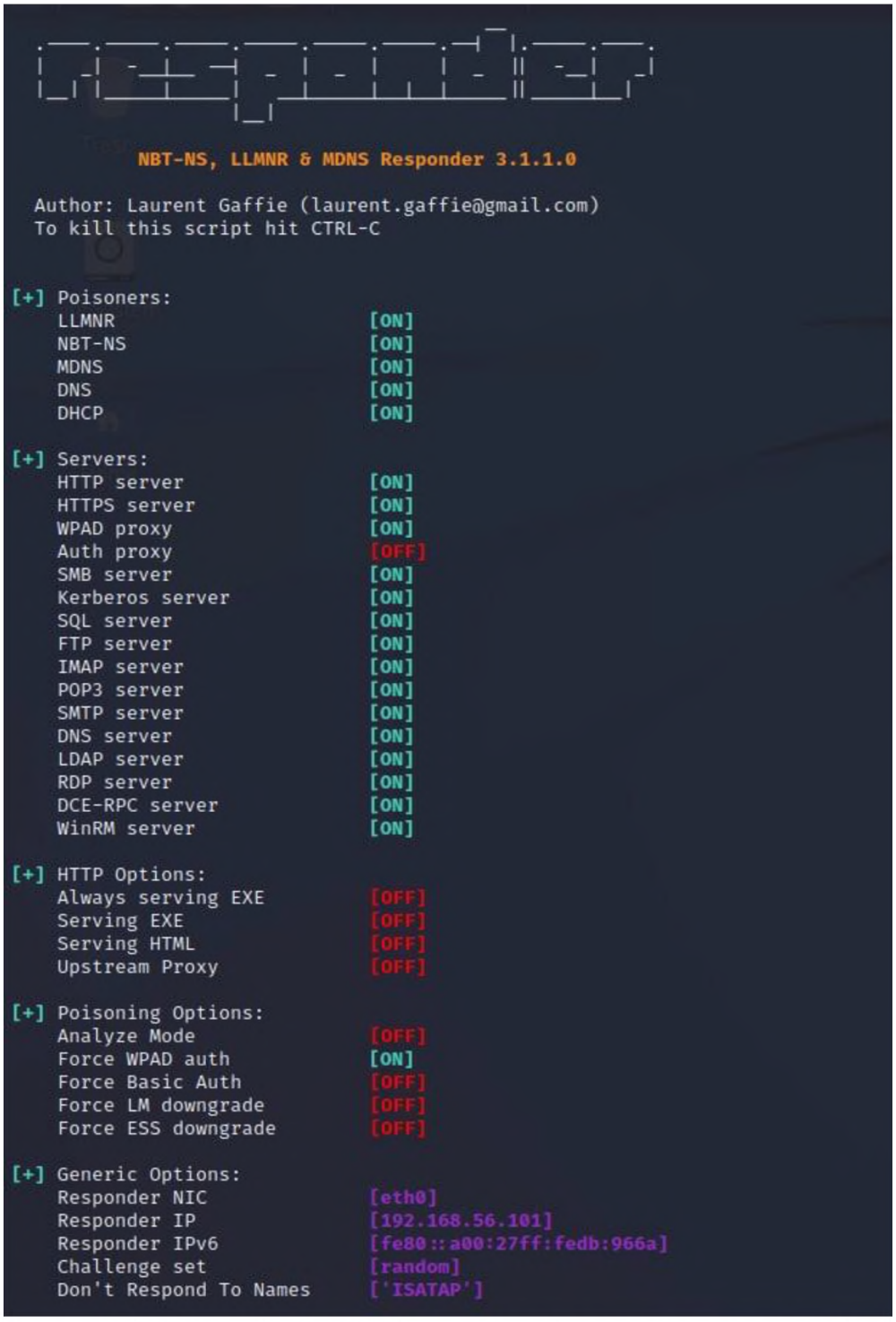


Рисунок 1.2 Інтерфейс ПЗ Responder після запуску з переліком діючих функцій

Після запуску Responder на рисунку 1.2 можна побачити усі запущені отруйники та сервери. Як приклад буде розглянута атака за допомогою отруєння запиту на підключення до SMB серверу.

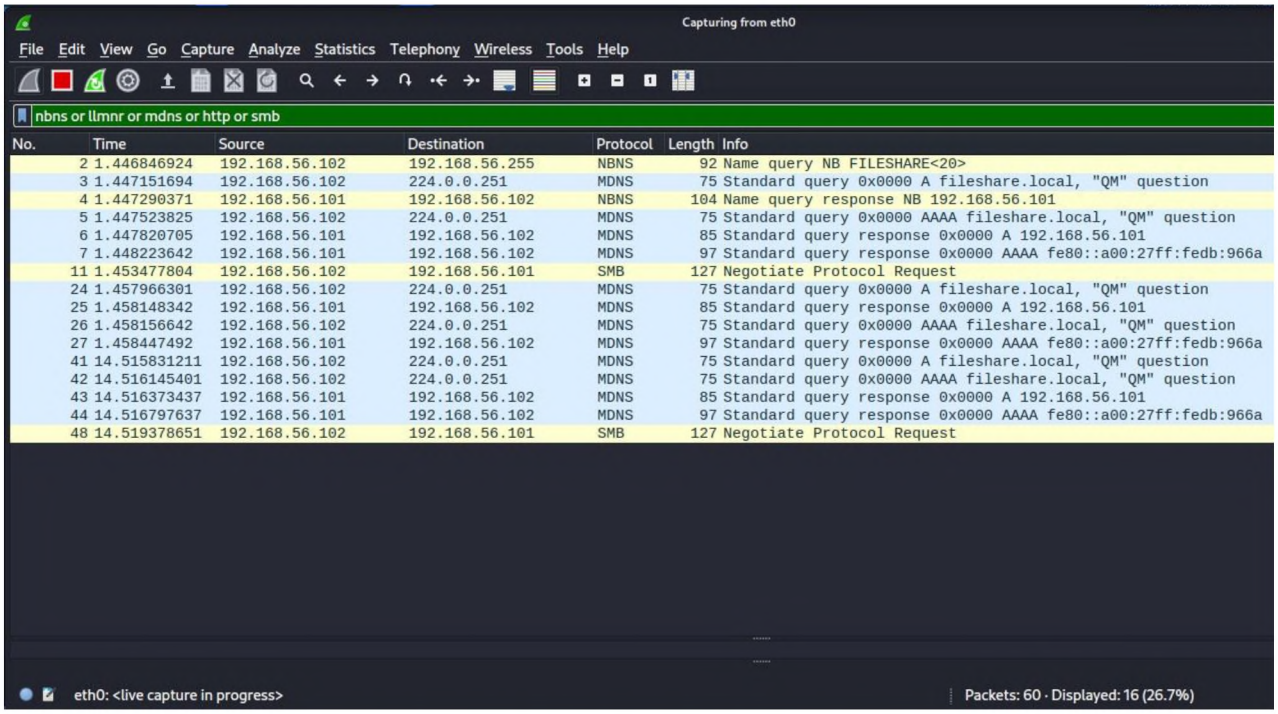


Рисунок 1.3 Перехоплення мережевих пакетів під час атаки у ПЗ Wireshark [8]

1. Користувач намагається підключитися до будь-якого файлового серверу який не існує, через помилку у назві цього серверу або у разі якщо файлового серверу у мережі взагалі немає. Машина при цьому надсилає мультікаст запити по всій локальній мережі – пакети номер два и три на рисунку 1.3.

2. Так як такого файлового серверу у дійсності немає, Responder відповідає машині користувача затверджуючи що він і є шуканим файловим сервером – пакети номер чотири, шість та сім на рисунку 1.3.

3. Машина користувача надсилає запит за з'єднання з файловим сервером SMB на машині з Responder – пакет номер 11 на рисунку 1.3. Та Responder надає згоду.

4. Користувач приєднується до шкідливого файлового серверу та отримує запит з проханням ввести дані облікового запису, як можна побачити на рисунку 1.4.

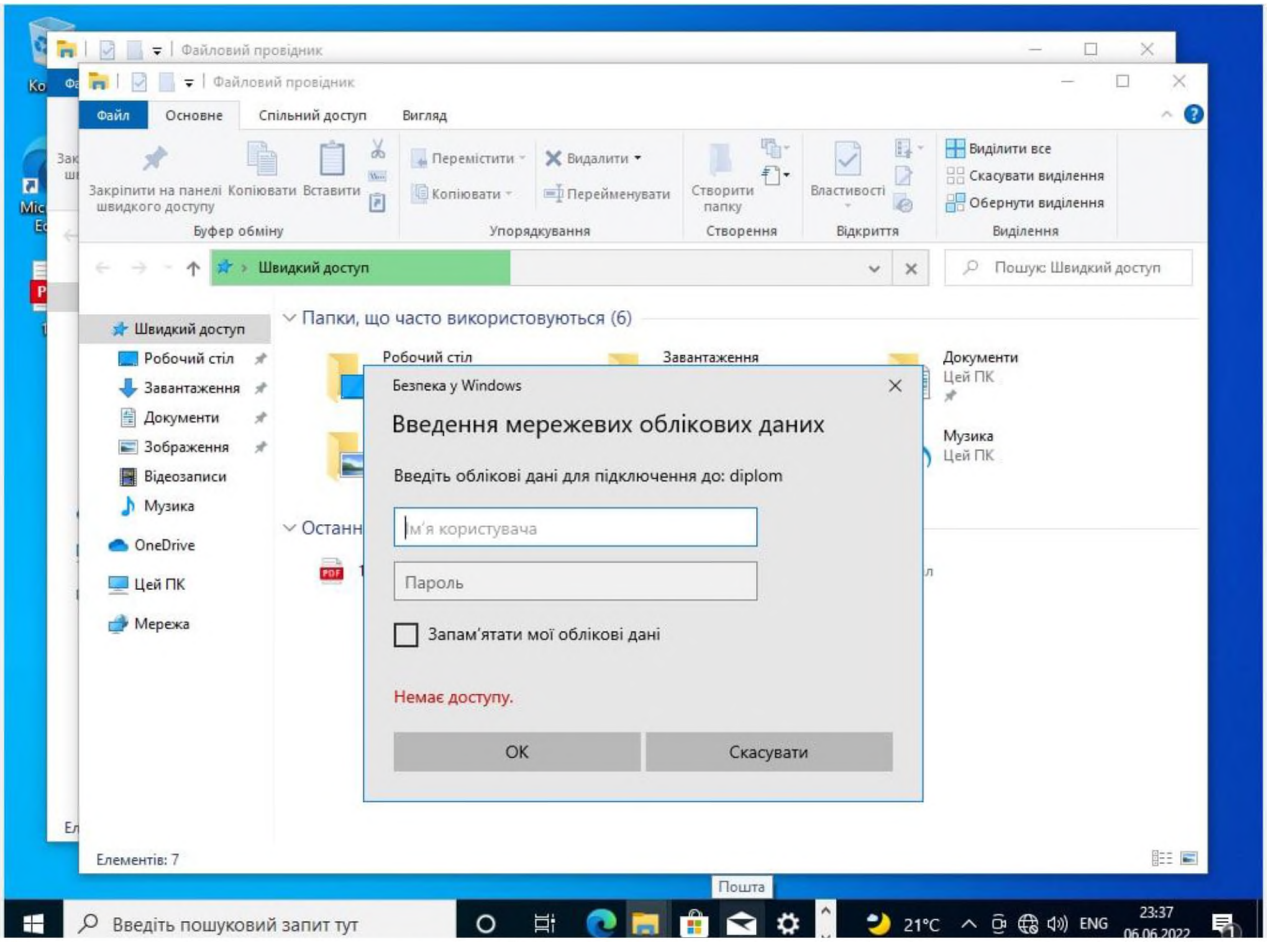


Рисунок 1.4 Приклад запиту облікових даних на робочій станції від шкідливого серверу

5. Користувач надає свої облікові дані, машина відправляє ім'я користувача та хешований пароль серверу та Responder їх отримує – рисунок 1.5.

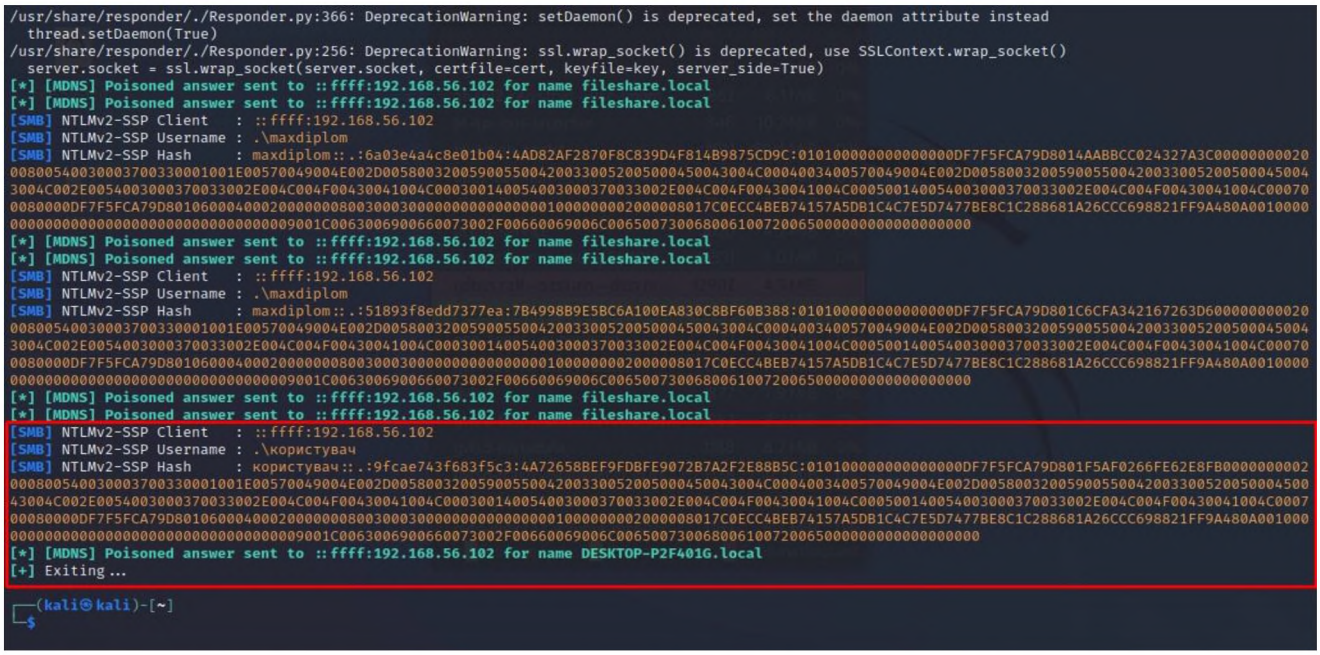


Рисунок 1.5 Приклад облікових даних користувача що отримує ПЗ Responder

Після отримання облікових даних та хешованого пароля, зловмисник може підключитися до справжнього файлового серверу. Також зловмисник має можливість зламати хеш за допомогою стороннього ПЗ, у тому числі і безкоштовного, та отримати пароль. Також знаючи точне ім'я користувача можливо провести атаку грубою силою та перебором отримати пароль.

Це тільки один із способів атаки за допомогою отруєння. Як видно на рисунку 1.2, передбачено багато інших методів атаки, у тому числі ті які не потребують чекати доки користувач зробить помилку у назві. Наприклад отруєння за допомогою протоколу WPAD з примусовою аутентифікацією, що запитає користувача його облікові дані просто після запуску веб-браузера. При цьому ніяких налаштувань зі сторони зловмисника непотрібно – усе що було необхідно зробити для скоєння атаки це скачати та встановити загальнодоступний безкоштовний образ системи, та запустити ПЗ Responder однією командою у терміналі.

1.3 Аналіз ІТС у якої знаходиться робоча станція.

Об'єктом дослідження є робоча станція коллцентра банківської установи. Через те що це коллцентр саме банківської установи, оператори цього коллцентру виконують не тільки дзвінки, як у звичайному коллцентрі, я й займаються перевіркою документів клієнтів та їх транзакцій. У коллцентрі працює близько 600 операторів. Робочі станції знаходяться у, захищеному від зовнішнього вторгнення неавторизованих персон, 9-поверховому офісному приміщенні, під постійним відео спостеріганням. У офісі знаходяться 400 робочих станцій.

Робоча станція являє собою персональний комп'ютер на базі операційної системи Windows та під'єднана до серверів Windows Active Directory та Windows Server Update Service.

Аутентифікація користувача здійснюється за допомогою LDAP серверу з застосуванням TLS шифрування.

Доступ до внутрішньої мережі банка та робочих комплексів які у неї знаходяться відбувається через зашифрований канал після аутентифікації на

робочій станції та подальшої двухфакторної аутентифікації користувача у програмному забезпечені VPN.

Оператор працює з персональними даними клієнтів банку, роблячи у процесі знімки екрану (для уточнення питання або для завантаження у банківські комплекси для звітності). Тобто предметом інтересу зловмисника можуть бути наступні речі:

- Облікові дані оператора для подальшого доступу до банківських комплексів;
- Записи та знімки екрану, які знаходяться на робочій станції оператора;
- Будь-який спосіб спостерігання за екраном оператора у процесі роботи.

Необхідно перевірити існуючи рішення щодо захисту від витоку інформації з робочої станції оператора коллцентра банківської установи та запровадити нові задля усунення існуючих вразливостей що можуть привести до витоку інформації та доповнення вже реалізованих заходів.

Також стоїть питання вибору оптимальної ОС з найменшою кількістю вразливостей зі сторони рядового користувача. У поточній конфігурації використовується ОС Windows, її необхідно порівняти з ОС Ubuntu у наступних аспектах:

- вбудовані вразливості ОС;
- сумісність з ПЗ яке використовуються у робочому процесі;
- зручність користування для робітника банку;
- складність налаштування та імплементації.

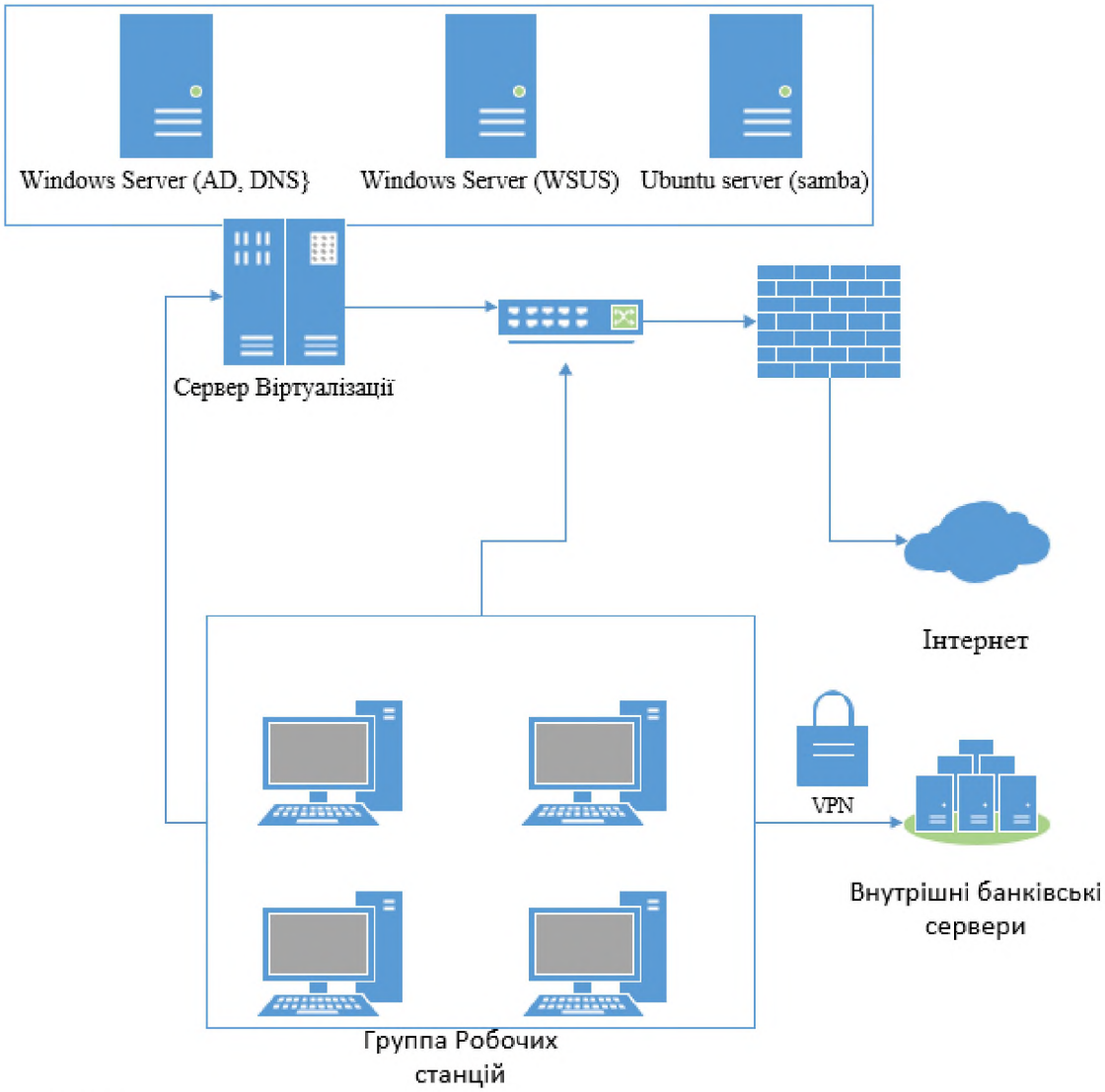


Рисунок 1.6 Спрощена схема мережі колцентру

Як показано на рисунку 1.6, крім самих робочих станції у локальній мережі також присутній сервер віртуалізації. На ньому знаходяться 3 сервери, з якими взаємодія робоча станція:

- Windows server з ролями Active Directory Domain Service та DNS серверу - Active Directory зберігає інформацію про об’єкти в мережі і робить цю інформацію для адміністраторів і користувачів легкою для пошуку та використання. Active Directory використовує сховище структурованих даних як основу для логічної, ієрархічної організації інформації каталогу. Наприклад, AD може зберігати облікові дані користувачів щоб виступати у ролі сервера аутентифікації на робочій станції та виступати у ролі контролера домену дозволяючи масово застосувати налаштування на усі під’єднані до цього домену робочі станції. У

поточній конфігурації використовується саме для застосування групових політик, так як аутентифікація не є кроссплатформною, тобто працює тільки на одній платформі – ОС Windows та незручна у імплементації і використанні;

- Windows server з роллю WSUS - Windows Server Update Services надає функції, які можна використовувати для керування та розповсюдження оновлень через консоль керування. У поточній конфігурації виступає джерелом оновлення – локальним сховищем оновлень. Завдяки цьому оновлення для робочих станцій буде завантажено з серверів Microsoft тільки один раз і буде далі поширюватися на робочі станцій у локальній мережі з серверу WSUS, що сильно знижує навантаження на мережу;
- Ubuntu server з Samba сервером – сервер на базі ОС Ubuntu server на якому розгорнутий файловий сервер Samba на базі мережевого протоколу SMB. Виступає як мережеве сховище необхідних для праці файлів для користувачів, адміністраторів та як сховище установників програм, які завдяки груповим політикам AD автоматично розгортаються на робочих станціях.

Доступ з робочої станції до інтернету відбувається через брандмауер, а до внутрішньої банківської мережі тільки через шифрований VPN канал після аутентифікації користувача як показано на рисунку 1.7.

Користувачу для аутентифікації у робочій станції необхідно знати логін та пароль свого облікового запису. Після того як користувач їх вводить, робоча станція з'єднується по зашифрованому каналу с сервером аутентифікації, де зберігаються дані облікових записів операторів (до аутентифікації користувача у VPN робоча станція може з'єднуватися з банківським сервером аутентифікації, але не з іншими внутрішніми серверами).

Після аутентифікації у системі робочої станції користувачу також необхідно аутентифікуватися у ПЗ VPN. На відміну від аутентифікації у системі робочої станції, авторизація у VPN двох факторна і для цього окрім даних облікового запису оператора також потрібен разовий пароль з смартфона оператора. І тільки після того як встановлюється шифрованих канал VPN, робоча станціє отримує доступ до решти банківських серверів та робочих комплексів.

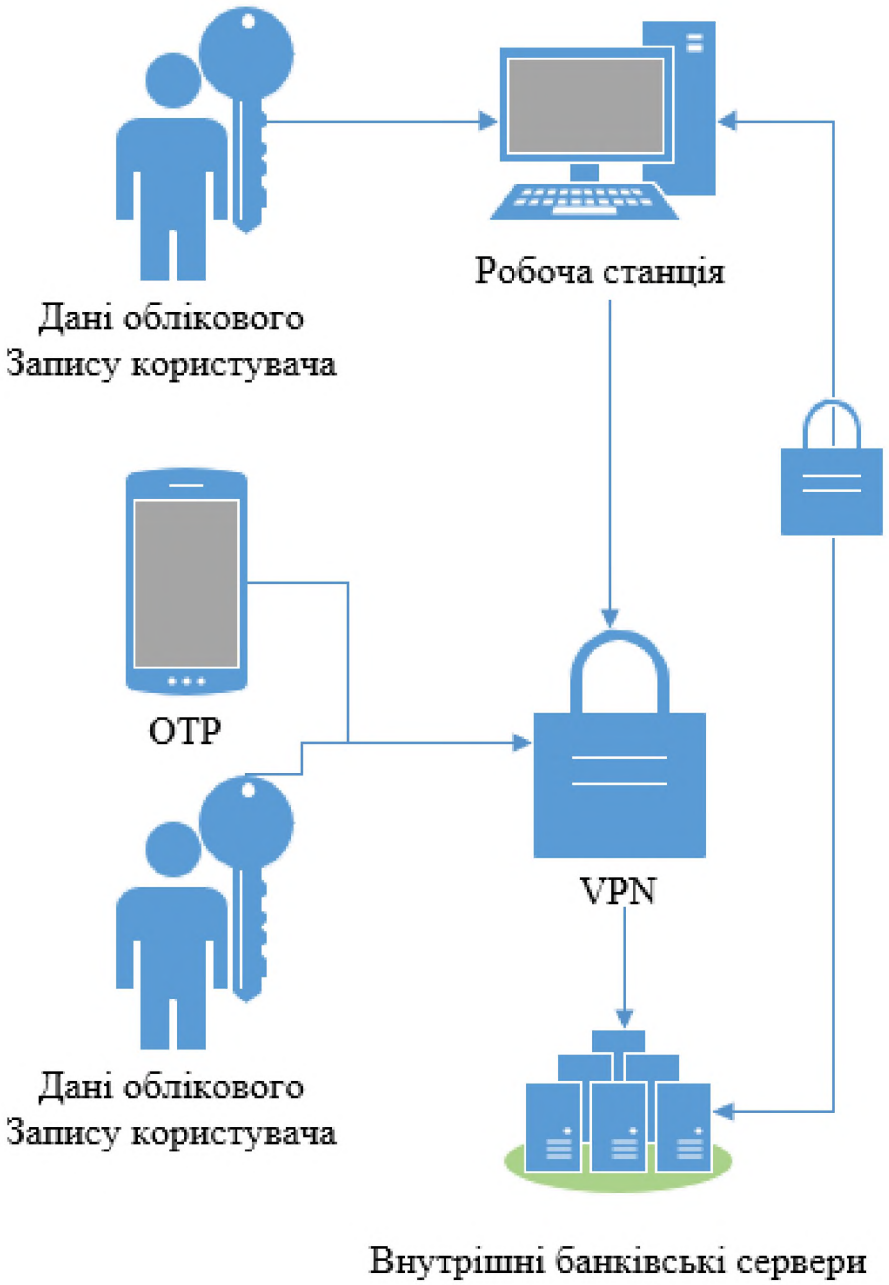


Рисунок 1.7 Схема процесу аутентифікації користувача робочої станції

1.4 Вибір оптимальної ОС для робочого ПЗ

У даному коллцентрі розглядається можливість переходу з ОС Windows на ОС на базі Linux, так як вона вважається не такою вразливою та більшість дистрибутивів Linux систем розповсюджується по ліцензії з відкритим кодом,

тобто є безкоштовними. Тому необхідно порівняти статки та недоліки ОС Windows яка використовується зараз та ОС на базі Linux, зокрема ОС Ubuntu.

1.4.1 Безпечність використання ОС Windows та ОС Linux

У таблиці 1.1 порівнянні вбудовані особливості двох ОС та їх відмінності, які будуть далі розглянуті докладніше [9], [10].

Таблиця 1.1 - Порівняння особливостей ОС Windows та ОС на базі Linux

Особливість ОС	Windows	Linux
LLMNR	Включений за замовчуванням	Виключений за замовчуванням
NetBIOS	Включений за замовчуванням	Відсутній за замовчуванням
WPAD	Включений за замовчуванням	Виключений за замовчуванням
Сегментованість файлового простіру	Не сегментований	Сегментований
Розповсюдженість використання	~75-80% в усьому світі	~3-5% в усьому світі
Відкритість коду	Закритий	Відкритий
Адміністративні привілеї	За замовчуванням надаються користувачу	Використається окремий обліковий запис з адміністративними привілеями
Мінімальна версія SMB	SMBv1	SMBv2

LLMNR, NetBIOS, WPAD – це застаріли та небезпечні мережеві протоколи визначення імен, за допомогою яких не складає праці здійснити атаки типу спуфінг та людина посередні, в результаті яких зловмисник зможе

перенаправляти запити машини користувача на шкідливі налаштовані сервери зловмисника замість справжніх та вкрасти облікові дані користувача у процесі. Ці протоколи увімкнені за замовчанням у ОС Windows, але у ОС Ubuntu вони або вимкнені або не присутні взагалі. Детальніше ці вразливості буде розглянуто у другої частині.

Сегментованість файлового простору – у ОС Linux файловий простір, на відміну від ОС Windows, у кожного користувача окремий та відокремлений від файлового простору де знаходяться системні файли. Через це атака яка знищує чи пошкоджує файловий простір, скоріш за все пошкодить тільки простір самого користувача та не зачепить системні файли та директорії, коли атака на файловий простір ОС Windows з більшою вірогідністю призведе до непрацездатності всієї системи.

Розповсюдженість використання – тільки 3-5% персональних комп'ютерів використовує ОС на базі Linux. Це приводить до того що майже все шкідливе ПЗ виробляється виключно з ціллю атаки на ОС Windows, бо пошук вразливостей та розробка такого ПЗ займає багато часу, а в випадку з ОС Linux вірогідність потрапити на комп'ютер саме з цією ОС складає лише 3-5%. Ускладняються це ще й тим що ОС на базі Linux скоріш за все буде використовувати технічно освічена людина, що ще більше знижує шанс успішної атаки.

Відкритість вихідного коду – код ядра Linux та більшості дистрибутивів, побудованого на ньому – відкритий, на відміну на ОС Windows. Тобто у разі ОС Linux пошуком та навіть усуненням вразливостей може займатися необмежена кількість людей, коли у випадку ОС Windows цим займається тільки дуже обмежене коло співробітників Microsoft. Це не тільки стримує темп пошуку та усунення вразливостей, але й не дає користувачам самостійно розробляти та застосовувати оновлення та виправляння безпеки.

Адміністративні привілеї – ОС Linux слідує філософії мінімально необхідних привілеїв, у той час як ОС Windows за замовчуванням видає повні адміністративні привілеї користувачу. Це стримує неосвічених користувачів від

встановлення та запуску більшості шкідливого ПЗ та від пошкодження системних файлів.

Мінімальна версія SMB - протокол SMB є один із самих розповсюджених методів створення файлового серверу. У той час як останні версії цього протоколу – SMBv2 та SMBv3 є досить безпечними, а у випадку SMBv3 ще й з вбудованим шифруванням, SMBv1 є застарілою та дуже небезпечною. Та на відміну від ОС на базі Linux, SMBv1 підтримується ОС Windows та увімкнений за замовчанням. Це є серйозною загрозою небезпеки, як показано у пункті 1.5.

1.4.2 Загальні особливості

Для тесту був обраний дистрибутив Ubuntu версії 20.04. Розгорнути обидві ОС системи не складає праці, засоби для масового розгортання вже налаштованих образів ОС також присутні для обох ОС та легкі у використанні. Для розгорнення ОС Windows використовувалося ПЗ Aomei Backupper, для ОС Linux було обрано ПЗ з відкритим кодом Clonezilla.

Стандартна графічна оболонка та методи налаштування та керування ОС на базі Linux є дуже незвичними та ворожими для користувача який звик до ОС Windows, бо майже усі просунуті операції у ОС на базі Linux виконуються завдяки терміналу, коли у ОС Windows вони виконуються завдяки графічного інтерфейсу ОС. У разі рядового користувача це є великою перешкодою, але так як усі налаштування виконуються системними адміністраторами, у цьому випадку це не стало проблемою. Стандартну графічну оболонку Gnome було замінено на графічну оболонку KDE, яка набагато більш схожа з оболонкою ОС Windows. Після додаткових декоративних налаштувань, був проведений тест по підсумкам якого оператори які користувалися тільки ОС Windows не мали ніяких перешкод з користуванням та навігацією по системі.

ОС на базі Linux також відрізняються швидкодією завдяки набагато більш організованій файловій системі та легковісності. На практиці це не вплинуло на процес роботи оператора, але скоротило час розгортання системи на порожню робочу станцію. Додаткову завдяки тому що ОС на базі Linux не потрібно приєднувати до доменного серверу AD час розгортання скоротився ще сильніше,

коли у разі ОС Windows це потрібно робити вручну на кожній машині, кожного разу як ОС станції перевстановлюється, що потребує перевантаження машини та займає додатково 5-10 хвилин на машину. Для масового налаштування та розгортання ПЗ на ОС Linux було обрано безкоштовне ПЗ Webmin, яке є аналогом AD, але дозволяє встановити сертифікат домену та налаштувати підключення до домену у зображенні системи перед розгортанням.

1.4.3 Сумісність

Те що ОС на базі Linux використовується тільки 3-5% персональних комп'ютерів хоч и робить для зловмисників розробку шкідливого ПЗ невигідним, що є великою перевагою, це також робить розробку звичайного ПЗ невигідним для звичайних законослухняних дистриб'юторів ПЗ. Це приводить до того що велика кількість ПЗ яке використовується на ОС Windows є недоступною на ОС на базі Linux. Але для ОС на базі Linux розроблено багато альтернатив такого ПЗ, яке зазвичай ще й ж безкоштовне. На додачу к цьому спеціально присутній програмний прошарок Wine та ПЗ на його основі, яке дозволяє інсталювати та запускати ПЗ ОС Windows на машині під керуванням ОС на базі Linux.

У компанії присутній відділ роботи з клієнтами, у якому операторами використовується ПЗ для VOIP телефонії, яке не має дистрибутиву для ОС на базі Linux та відділ керуючий телефонією відмовився переходити на аналогічне ПЗ забезпечення, яке має дистрибутиви для ОС на базі Linux. Тому був обраний другий метод – використання програмного прошарку Wine.

Тестування показало, що усе ПЗ та робоча станція на ОС Linux взагалі є працездатною та у операторів не виникло проблем з її використанням. Але використання програмного прошарку Wine призвело до сильного, у порівнянні з ОС Windows, навантаження робочої станції, що у деяких випадках зашкоджувала роботі операторів. На додаток к цьому виявилося що близько половини робочих станції поставили з відмінними апаратними складовими - в них присутні застаріли моделі відеокарт, для яких немає відповідних драйверів та ПЗ, що зробило половину робочих станції непрацездатними при використанні ОС на базі Linux. Про відмінність апаратних складових керівництво компанії не знало, а від

платного ПЗ на базі програмного прошарку Wine, на якому ПЗ все ж таки працювало, керівництво відмовилось. Тому після довгого процесу налаштування и тестування керівництво відмовилось від переходу на ОС на базі Linux та у спеціальній частині буде проведено виявлення та усунення вразливостей у ОС Windows, яка використовується у поточній конфігурації та буде продовжувати використовуватися.

1.5 Усунені загрози витоку інформації з робочої станції

1.5.1 Крадіжка облікових даних

Викрасти дані облікового запису можна декількома методами. Один з них це крадіжка даних через атаку безпосередньо на оператора - методом фішингу, соціальної інженерії, зламом персонального комп'ютера або смартфона оператора. Для запобігання подібного витоку інформації усім операторам при прийомі на роботу та на регулярній основі проводяться тренінги по кібербезпеці та безпечному користуванні та роботі у мережі інтернет.

Другий спосіб це крадіжка даних під час аутентифікації оператора у робочій станції. Таку атаку теж можна виконати декількома способами. Це прослуховування пакетів у мережі де знаходиться робоча станція та атака типу spoofing або man-in-the-middle, тобто змусити робочу станцію передавати облікові дані на спеціально налаштований сервер зловмисника замість справжнього сервера аутентифікації.

Аутентифікацію на робочій станцій відбувається за допомогою налаштованого серверу на базі протоколу LDAP - програмний протокол, який дозволяє знаходити дані на сервері про організацію, окремих осіб та інші ресурси, такі як файли та пристрої в мережі. У поточній конфігурації він виступає сервером зберігання облікових даних операторів та сервером аутентифікації. На відміну від аутентифікації через засоби AD, він є кросплатформним та дозволяє під'єднати аутентифікацію не тільки для ОС робочої станції а й програмних комплексів.

Щоб запобігти вищеназваним атакам, при з'єднані з сервером використовується SSL/TLS сертифікати, які забезпечують шифрування пакетів у

яких передаються облікові дані оператора, тобто при прослуховуванні зловмисник зможе отримати тільки марні зашифровані дані з яким без приватного ключа серверу аутентифікації він нічого не зможе зробити. Використання сертифікатів також запобігають тому щоб робоча станція з'єднувалась не з справжнім сервером аутентифікації завдяки перевірці автентичності сертифікатів.

1.5.2 Неавторизований доступ

У випадку якщо зловмисник зміг отримати дані облікового запису оператора завдяки фішингу, соціальної інженерії або іншими методами, йому все одно потрібно отримати доступ до робочої станції. Як було зазначено у пункті 1.1, це є непростою задачею через декілька причин:

- Вхід у будівлю де знаходиться робоча станція відбувається за допомогою біометричних даних оператора та через пункт охорони;
- Навіть якщо зловмисник зможе потрапити у будівлю офісу, йому потрібне буде знати де саме знаходиться станція цього конкретного оператора, а у багатоповерховій будівлі де знаходиться більш ніж 400 робочих станцій, вгадати це неможливо;
- Оператори згідно з робочими інструкціями повинні наприкінці зміни видаляти усі знімки екрану та відеозаписи. ОС робочих станції також регулярно скидається та оновлюється, видаляючи у процесі всі локальні дані користувачів;
- З технічного боку оператор може працювати на будь-якій робочий станції з чотирьохсота, враховуючи що багато операторів працює змінами 2 через два дні, якщо бажаний оператор не працює у цей день, дуже велика ймовірність того що робоча станція буде окупована іншим оператором;
- Людина яка буде ходити по усім поверхам та робочим станціям у будівлі буде викликати підозру у операторів які працюють у офісі;
- Якщо зловмисник зможе отримати доступ до порожньої робочої станції, він все одно не зможе отримати доступ до банківських робочих комплексів, так як для доступу до них необхідно аутентифікуватися у ПЗ VPN за допомогою разового паролю, який генерується у смартфоні оператора;

- Робоча станція та будівля знаходиться під цілодобовим відеоспостереженням, вхід у будівлю через біометричні дані та сеанси користувачів на робочих станція записуються у логи та зберігаються. Встановити особу зловмисника не складе праці.

Як можна побачити, навіть якщо зловмисник зміг отримати облікові дані оператора, получити доступ до потрібної робочої станції є практично неможливою задачею. Та навіть у разі вдалої спроби проникнення, відслідкувати та визначити особу зловмисника, буде дуже легко.

1.6 Висновок до першої частини

Як можна побачити, вразливості при використанні ОС Windows є досить серйозними бо дозволяють вкрасти облікові дані або перенаправляти користувача робочої станції на шкідливі мережеві ресурси та сервери зловмисника замість справжніх, та при цьому реалізувати атаки, використовуючи вбудовані та увімкнені за замовчанням вразливості, не складає праці і це може зробити кожний бажаючий. Якщо враховувати ще й те що 75% усіх користувачів у світі використовують саму цю ОС як у персональному так і у комерційному секторі, це робить використання цих вразливостей дуже привабливим для зловмисників. Через це усунення цих вразливостей є дуже важливим для будь-якого користувача ОС Windows.

Також у розділі було описано процес порівняння ОС Windows, що використовується у поточній конфігурації, та ОС на базі Linux яку було запропоновано як більш безпечну альтернативу, але яка після довгого процесу налаштування не пройшла перевірку на сумісність з поточним обладнанням та ПЗ.

Метою другого розділу є аналіз загроз характерних для персональних комп'ютерів під керуванням ОС Windows. Необхідно виявити вразливості у налаштуванні робочих станцій, проаналізувати загрози що через них реалізуються та запропонувати методи їх усунення.

Для забезпечення безпеки інформації, яка знаходиться на робочої станції необхідно запровадити:

- Захист від атак через шкідливе ПЗ;
- Захист від витоку інформації за допомогою зовнішніх носіїв інформації;
- Захист від витоку інформації з внутрішнього носія інформації робочої станції;
- Захист від вразливостей через некоректне налаштування програмного забезпечення робочої станції.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Усунення вразливостей мережевих протоколів ОС

2.1.1 Усунення вразливостей протоколів визначення імен.

У мережі офісу було проведено пентест за допомогою безкоштовного ПЗ з відкритим кодом у вигляді дистрибутиву ОС Linux – Kali. Пентест показав що всі робочі станції у мережі є вразливими для атак через вбудовані у ОС Windows застарілі мережеві протоколи, які є частиною ОС Windows та увімкнені по стандарту після розгорнення системи задля забезпечення зворотної сумісності з застарілим обладнанням яке не спроможне використовувати сучасні версії цих протоколів або взагалі нові які прийшли їм на заміну.

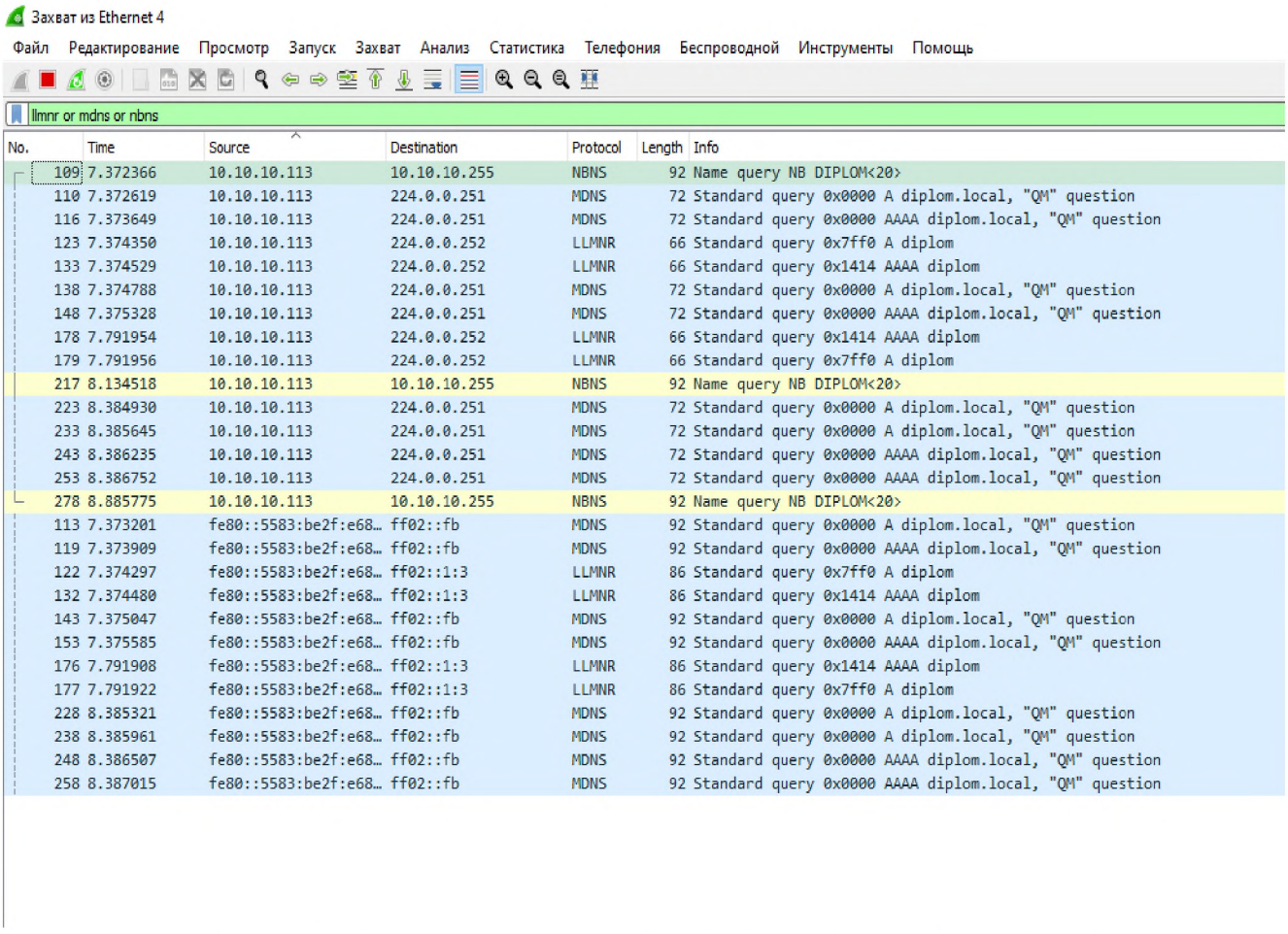
Ці протоколи є протоколами Name Resolution (протоколи визначення імені) – які використовуються системою для того щоб визначити IP адресу за допомогою її імені хоста.

На машині під керуванням ОС Windows процес виглядає так:

1) Система отримує ім’я хоста та вимагає його IP адресу для підключення;
2) Перевіряється локальний файл зі списком хостів та їх адресами;
3) Якщо у локальному списку такого хоста не знайдено, система звертається до локального кешу DNS у якому знаходиться інформація щодо нещодавно визначених хостів;
4) Коли бажаного ім’я хосту не знаходиться и у локальному кешу DNS, система посилає запит у налаштований DNS сервер;
5) Якщо усі попередні шаги не дали бажаного результату – машина посилає мультікаст запит (запит по мультікаст адресі ***.***.***.255 який спрямований до усіх пристроїв у мережі) щоб перевірити чи є у них запис щодо цього хоста.

Як можна побачити, фінальний крок для визначення адреси хоста використовує мультікаст визначення імен. Він керований трьома головними протоколами: NBT-NS (NetBIOS Name Service), LLMNR (Link-Local Multicast Name Resolution) та mDNS (multicast DNS).

Три протоколи використовуються одночасно задля забезпечення максимальної сумісності та підтримки застарілих пристроїв. При цьому NBT-NS був створений у ранніх 80-х роках та не відповідає сучасним стандартам безпеки. Коли протокол став втрачати популярність, машини на ОС Windows почали використовувати наслідника NBT-NS – LLMNR (який все одно підтримує NBT-NS для комунікації з застарілими пристроями). Приклад можна побачити на рисунку 2.1.



No.	Time	Source	Destination	Protocol	Length	Info
109	7.372366	10.10.10.113	10.10.10.255	NBNS	92	Name query NB DIPLOM<20>
110	7.372619	10.10.10.113	224.0.0.251	MDNS	72	Standard query 0x0000 A diplom.local, "QM" question
116	7.373649	10.10.10.113	224.0.0.251	MDNS	72	Standard query 0x0000 AAAA diplom.local, "QM" question
123	7.374350	10.10.10.113	224.0.0.252	LLMNR	66	Standard query 0x7ff0 A diplom
133	7.374529	10.10.10.113	224.0.0.252	LLMNR	66	Standard query 0x1414 AAAA diplom
138	7.374788	10.10.10.113	224.0.0.251	MDNS	72	Standard query 0x0000 A diplom.local, "QM" question
148	7.375328	10.10.10.113	224.0.0.251	MDNS	72	Standard query 0x0000 AAAA diplom.local, "QM" question
178	7.791954	10.10.10.113	224.0.0.252	LLMNR	66	Standard query 0x1414 AAAA diplom
179	7.791956	10.10.10.113	224.0.0.252	LLMNR	66	Standard query 0x7ff0 A diplom
217	8.134518	10.10.10.113	10.10.10.255	NBNS	92	Name query NB DIPLOM<20>
223	8.384930	10.10.10.113	224.0.0.251	MDNS	72	Standard query 0x0000 A diplom.local, "QM" question
233	8.385645	10.10.10.113	224.0.0.251	MDNS	72	Standard query 0x0000 A diplom.local, "QM" question
243	8.386235	10.10.10.113	224.0.0.251	MDNS	72	Standard query 0x0000 AAAA diplom.local, "QM" question
253	8.386752	10.10.10.113	224.0.0.251	MDNS	72	Standard query 0x0000 AAAA diplom.local, "QM" question
278	8.885775	10.10.10.113	10.10.10.255	NBNS	92	Name query NB DIPLOM<20>
113	7.373201	fe80::5583:be2f:e68…	ff02::fb	MDNS	92	Standard query 0x0000 A diplom.local, "QM" question
119	7.373909	fe80::5583:be2f:e68…	ff02::fb	MDNS	92	Standard query 0x0000 AAAA diplom.local, "QM" question
122	7.374297	fe80::5583:be2f:e68…	ff02::1:3	LLMNR	86	Standard query 0x7ff0 A diplom
132	7.374480	fe80::5583:be2f:e68…	ff02::1:3	LLMNR	86	Standard query 0x1414 AAAA diplom
143	7.375047	fe80::5583:be2f:e68…	ff02::fb	MDNS	92	Standard query 0x0000 A diplom.local, "QM" question
153	7.375585	fe80::5583:be2f:e68…	ff02::fb	MDNS	92	Standard query 0x0000 AAAA diplom.local, "QM" question
176	7.791908	fe80::5583:be2f:e68…	ff02::1:3	LLMNR	86	Standard query 0x1414 AAAA diplom
177	7.791922	fe80::5583:be2f:e68…	ff02::1:3	LLMNR	86	Standard query 0x7ff0 A diplom
228	8.385321	fe80::5583:be2f:e68…	ff02::fb	MDNS	92	Standard query 0x0000 A diplom.local, "QM" question
238	8.385961	fe80::5583:be2f:e68…	ff02::fb	MDNS	92	Standard query 0x0000 A diplom.local, "QM" question
248	8.386507	fe80::5583:be2f:e68…	ff02::fb	MDNS	92	Standard query 0x0000 AAAA diplom.local, "QM" question
258	8.387015	fe80::5583:be2f:e68…	ff02::fb	MDNS	92	Standard query 0x0000 AAAA diplom.local, "QM" question

Рисунок 2.1 Приклад того як виглядає запити робочої станції у ПЗ Wireshark

NBT-NS, LLMNR та mDNS транслюють запит у всю внутрішню мережу, але ніяких дії щоб перевірити відповідь не застосовується. Зловмисники можуть експлуатувати цей механізм слухаючи подібні запити та підробляючи відповіді –

змушуючи жертву довіряти шкідливим серверам. Зазвичай ця довіра буде використовуватися щоб вкрасти логіни и паролі жертви.

Усугубляє ситуацію те що розроблено та знаходиться у вільному доступу безліч інструментів які автоматично прослуховують мережу на наявність таких запитів та у той же час не потребують поглибленого знання роботи мережі чи цих протоколів для розгорнення, експлуатації та завдання шкоди.

Поширені випадки зловживання:

- Помилка при наборі – якщо користувач робить помилку у назві дійсно існуючого та надійного хоста, зазвичай відповідного запису у системі знайдено не буде та машина вдасться до багатоадресної передачі запитів для визначення хоста. Цей випадок досі слабкий, бо зловмиснику доведеться чекати доки користувач не зробить помилку;
- Неправильне налаштування – конфігурація як на стороні DNS серверу, так і на стороні робочої станції може призвести к проблемі з визначенням ім'я та змусить систему покладатися на багатоадресні запити щодо визначення імен;
- Протокол WPAD – якщо у веб-браузер настроєний на автоматичне визначення проксі-серверу (а це за замовчуванням так і є), він буде використовувати протокол WPAD для виявлення URL-адреси файлу конфігурації проксі. Щоб визначити URL адресу, WPAD буде здійснювати прохід через серію потенційних URL адрес та хост імен та с кожною спробою відкривати себе для спуфінгу;
- Веб-браузер – коли цільний словісний рядок вводиться у пошукову строку, браузеру потрібен спосіб щоб визначити чи є цій рядок пошуковим запитом або веб адресою. Браузер спочатку розглядає рядок як пошуковий запит і спрямовує користувача до обраної пошукової системи, але у той ж час перевіряє чи не є ця строка адресою хоста, намагаючись визначити її адресу. Деякі браузери мають вбудований захист – наприклад Google Chrome буде намагатися визначити декілька випадково згенерованих хост імен щоб точно перевірити що вони не визначаються – гарантуючи захист від атак через проколи визначення імен, які реагують на будь-які запити;

Зважаючи на те що багатоадресне визначення імен відбувається на рівні peer-to-peer (з'єднання між двома точками напряму у мережі), більшість методів боротьби буде сфокусовано на забезпечення безпеки кінцевої точки, а не покладатися лише на безпеку мережі.

Відключення LLMNR – LLMNR вимикається завдяки редактору групових політик по дорозі Політика локального комп'ютера > Конфігурація комп'ютера > Адміністративні шаблони > Мережа > Клієнт DNS. У нашому випадку, завдяки тому що комп'ютери у мережі під'єднанні до серверу адміністрування Active Directory, політика налаштовується на сервері та далі це налаштування автоматично оновлюється на усіх комп'ютерах під'єднаних до робочого домену [11].

Відключення NetBIOS через TCP/IP - NetBIOS через TCP/IP вимикається у налаштуваннях мережевого адаптера та не має відповідної групової політики. Тобто це легко зробити на одичній робочій станції, але неможливо це зробити напряму через сервер AD для масового налаштування. Але це також можна зробити за допомогою PowerShell скріпту, який у свою чергу вже можна надіслати з сервера усім під'єднаним до домену комп'ютерам.

2.1.2 Усунення вразливостей RDP протоколу

RDP — це власний протокол Microsoft, який забезпечує віддалені підключення до інших комп'ютерів, як правило, через TCP-порт 3389. Він забезпечує доступ віддаленого користувача до мережі через зашифрований канал. Адміністратори мережі використовують RDP для діагностики проблем, входу на сервери та виконання інших віддалених дій. Віддалені співробітники використовують RDP для входу в мережу організації для доступу до електронної пошти та файлів.

Зловмисники використовують неправильно налаштовані порти RDP, які відкриті для Інтернету, щоб отримати доступ до мережі. Потім вони можуть потенційно переміщатися по всій мережі, підвищувати привілеї, отримувати доступ до конфіденційної інформації та вилучати її, отримувати облікові дані або розгортати широкий спектр шкідливих програм. Цей популярний вектор атаки

дозволяє зловмисникам зберігати низький профіль, оскільки вони використовують законну мережеву службу, яка надає їм ті ж функції, що й будь-який інший віддалений користувач. Зловмисники використовують такі інструменти, як пошукова система Shodan, щоб сканувати Інтернет на наявність відкритих портів RDP, а потім використовувати методи перебору пароля для доступу до вразливих мереж. Зламані облікові дані RDP також широко доступні для продажу на темних ринках.

Рекомендації що надає MS-ISAC стосовно використання RDP:

Після оцінки середовища та проведення відповідного тестування скористайтеся груповою політикою, щоб вимкнути RDP. Якщо RDP необхідний для законних робочих функцій, рекомендується дотримуватися наведених нижче рекомендацій:

- Розмістить будь-яку систему з відкритим портом RDP (3389) за брандмауером і вимагайте від користувачів підключення VPN через брандмауер;
- Увімкніть надійні паролі, багатофакторну автентифікацію та політику блокування облікового запису, щоб захиститися від атак за допомогою перебору;
- Дозвольте підключення тільки певних надійних хостів.
- Якщо можливо, обмежте вхід у RDP авторизованими обліковими записами без адміністративних привілеїв. Дотримуйтесь принципу найменших привілеїв, гарантуючи, що користувачі мають мінімальний рівень доступу, необхідний для виконання своїх обов'язків;
- Реєструйте та переглядайте спроби входу в RDP на предмет аномальної активності та зберігайте ці журнали щонайменше 90 днів. Переконайтеся, що лише авторизовані користувачі мають доступ до цієї служби;
- Переконайтеся, що хмарні середовища дотримуються найкращих практик, визначених постачальником хмарних послуг. Після завершення налаштування хмарного середовища переконайтеся, що порти RDP не увімкнено, якщо вони не потрібні для бізнес-цілей;
- Увімкніть автоматичне оновлення Microsoft, щоб переконатися, що працюють останні версії клієнтського та серверного програмного забезпечення;

- Виконуйте регулярне сканування, щоб переконатися, що RDP залишається закритим від Інтернету.

Для нашої конфігурації служба RDP користувачам не потрібна, тому її треба просто відключити на усіх робочих станціях, це робиться за допомогою групової політики по шляху Конфігурація комп'ютера > Адміністративні шаблони > Компоненти Windows > Служби віддаленого робочого стола > Хост сеансу віддаленого робочого стола > Підключення.

У разі потреби підключення адміністратора до робочої станції, буде використовуватися ПЗ системи VNC з окремими обліковим записом, який не буде перетинатися з обліковим записом оператора та забезпечує повністю шифроване з'єднання між хостами та дозволяє використовувати двох-факторну автентифікацію.

2.1.3 Усунення вразливостей протоколу WPAD

WPAD — це протокол автоматичної конфігурації проксі-сервера. Цей протокол використовується клієнтами (браузерами) для визначення розташування (URL) розташування файлу конфігурації за допомогою технологій DHCP та/або DNS.

Під час запиту браузер викликає спеціальну функцію FindProxyForURL з файлу PAC, куди передається URL і хост. Очікувана відповідь – це список проксі-серверів, через які буде здійснюватися доступ до цієї адреси.

Розташування файлу конфігурації PAC можна визначити за допомогою DHCP, DNS або LLMNR. Зловмисники можуть використати вразливість у WPAD, вказавши розташування спеціально налаштованого файлу PAC, який буде перенаправлять запит браузера через проксі-сервери під контролем зловмисників.

Цього також можна досягти у відкритій бездротовій мережі шляхом зламу маршрутизатора або точки доступу, або шляхом відкриття доступу до спеціально налаштованої точки доступу для доступу всім.

При цьому немає абсолютно ніякої необхідності скомпрометувати власну мережу атакованого комп'ютера, оскільки система використовуватиме WPAD для виявлення проксі-серверів. Це є загрозою для будь-якого користувача ОС

Windows бо функція WPAD включена за замовчуванням на всіх комп'ютерах з операційною системою Windows.

Вимкнути цю функцію на усіх робочих станціях можна за допомогою групової політики по шляху Конфігурація користувача > Політики > Налаштування Windows > Автоматична конфігурація браузера > Автоматичне визначення параметрів конфігурації. Це запобіжить від автоматичного пошуку проксі серверів на робочій станції.

2.2 Усунення вразливостей через застосування SAMBA серверу у мережі

SMB – це мережевий протокол обміну файлами та ресурсами, що використовує модель клієнт-сервер. Клієнти SMB, такі як ПК у мережі, підключаються до серверів SMB для доступу до таких ресурсів, як файли та каталоги, або для виконання таких завдань, як друк через мережу.

Як працює SMB - на високому рівні SMB комунікацію досить проста. Клієнти SMB підключаються до сервера SMB, використовуючи порт SMB, для доступу до загальних ресурсів SMB. Отримавши доступ до загальних ресурсів SMB, клієнти можуть виконувати такі дії, як спільна робота над файлами, не завантажуючи їх на комп'ютери, або друкувати на мережному принтері.

У нашому випадку розгорнутий SAMBA сервер (мережевий сервер або кластер серверів, де зберігаються загальні ресурси SMB) на ОС Ubuntu. Сервер SMB надає або забороняє клієнтам SMB доступ до загальних ресурсів (також відомих як SMB share). З нього користувачі робочих станцій, виступаючи у цьому випадку SMB клієнтами, можуть завантажувати файли необхідні для роботи, у разі якщо вони не присутні на робочої станції.

Чи є безпечним SMB - як і у більшості мережевих протоколів, чи є SMB безпечним, залежить від його версії та реалізації. Взагалі, сьогодні SMB є дуже безпечним протоколом. Для сучасних реалізацій малого та середнього бізнесу є кілька ключових принципів захисту SMB:

- Не можна використовувати SMBv1. SMB1 не має шифрування, є неефективним і використовувався в безлічі атак програм-вимагачів;

- Треба віддавати перевагу SMB3 або новішій версії, коли це можливо. З трьох основних версій SMB, SMB3 — зокрема SMB 3.1.1 — забезпечує найбільшу безпеку. Наприклад, безпечне узгодження діалекту SMB3 обмежує сприйнятливість до атак «людина посередині» (MITM), а SMB 3.1.1 використовує безпечні та ефективні алгоритми шифрування, такі як AES-128-GCM;
- Необхідно обмежити доступ SMB до надійних мереж і клієнтів. Лише дозвіл підключення з надійних локальних мереж або клієнтів і впровадження жорстких політик безпеки мережі для доступу SMB може значно зменшити вашу атаки.

Версії SMB

SMB v1 (SMB1) - оригінальна версія SMB. SMB1 розпочався в 1980-х роках і пройшов кілька ітерацій. У Windows 95 Microsoft представила CIFS як спосіб реалізації SMB1. У сучасних програмах НЕ слід використовувати SMB v1, оскільки він небезпечний (немає шифрування, використовувався в таких атаках, як WannaCry і NotPetya) і неефективний (постійно надсилає велику кількість повідомлень у мережу, що створює перевантаження та знижує продуктивність).

SMB v2 (SMB2) - SMB2 було представлено в Windows Vista. Ця версія SMB має значні покращення в продуктивності та простоті порівняно з SMB1. Крім того, SMBv2 пропонує покращення безпеки. Наприклад, SMB2.0.2 представив цілісність попередньої аутентифікації, та SMB2 не вразливий до тих же експлойтів WannaCry і NotPeyta, які роблять SMB1 ризиком для безпеки. SMB версії 2.1 було представлено в Windows 7 і Server 2008 R2, та ще більше покращує продуктивність і впроваджує опортуністичне блокування (Opportunistic locking або також називається oplock — це блокування, що встановлюється клієнтом на файл, що знаходиться на сервері).

SMB версії 3 (SMB3) – SMB3, який представив наскрізне шифрування SMB, а пізніше є найдосконалішою та безпечною реалізацією SMB. Перший випуск SMB3 (він же SMB v3.0) вийшов з Windows 8 і Server 2012. SMB v3.02 був представлений у Windows 8.1 і Server 2012 R2. SMB 3.1.1 — останній протокол SMB — був представлений у Windows 10 і Server 2016.

Сервери SMB і клієнти SMB використовуватимуть останню версію, яку вони обидва підтримують. Таким чином, необхідно враховувати як серверне, так і клієнтське програмне забезпечення SMB під час захисту реалізацій SMB.

Підпис при доступі до SMB серверу – обов'язкова перевірка підпису SMB серверу також вмикається через налаштування групових політик по дорозі Конфігурація комп'ютера > Політики > Параметри Windows > Параметри безпеки > Локальні політики > Параметри безпеки.

2.2.1 Налаштування безпеки зі сторони Samba серверу

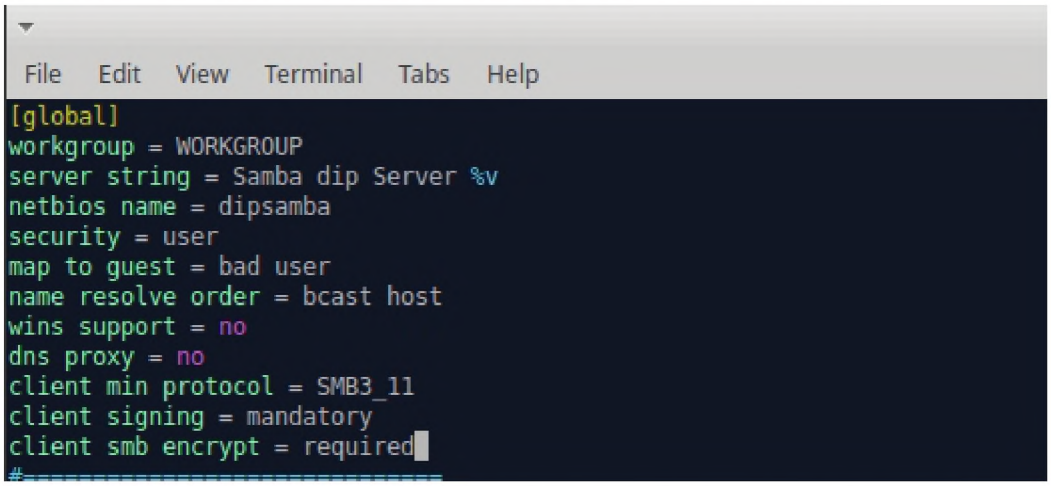


Рисунок 2.2 Файл конфігурації з налаштуваннями Samba серверу

Як можна побачити на рисунку 2.2, задля забезпечення безпечної роботи файлового Samba серверу застосовуються наступні налаштування:

Client min protocol - Цей параметр контролює мінімальну версію протоколу, яку клієнт намагатиметься використовувати. Встановлюється значення SMB3_11 – що відповідає останній найнадійніший версії SMB протоколу 3.11, яка імплементована у ОС Windows 10, яка використовується на робочих станціях. Це змусить клієнт використовувати саме цю версію Samba протоколу та заборонить доступ машинам шо будуть використовувати більш старі версії.

Client signing - Це визначає, чи дозволено клієнту вимагати від серверу підпис пакетів SMB протоколу, задля усунення можливості їх підробити. Значення встановлюється mandatory тобто підпис пакетів є обов'язковим.

Client smb encrypt - цей параметр визначає, чи повинен клієнт використовувати шифрування при зв'язку з SMB сервером. Значення встановлюється на required

тобто необхідно. Це не працює на старих версіях протоколу SMB, тому що в них відсутнє шифрування. Але у нашому випадку обов'язково використовується тільки остання версія SMB 3.11 і це змусить клієнт вимагати тільки зашифроване з'єднання.

2.2.2 Налаштування безпеки зі сторони Samba клієнту

Наступні два елементи політики застосовуються до клієнтів SMB, тобто до систем Windows, які підключаються до сервера SMB.

Мережевий клієнт Microsoft: цифровий підпис комунікацій (завжди)

Увімкнення цієї політики гарантує, що клієнт SMB завжди вимагатиме підписи пакетів SMB. Якщо сервер не згоден підтримувати підписання пакетів SMB із клієнтом, клієнт не зв'язуватиметься з сервером. За замовчуванням цю політику вимкнено, тобто SMB дозволено за замовчуванням без підпису пакетів. Як і раніше, можливе узгодження підписання пакетів, просто це не потрібно для роботи.

Мережевий клієнт Microsoft: цифровий підпис комунікацій (якщо згоден сервер)

Ця політика включена за замовчуванням і визначає, чи намагається клієнт SMB узгодити підписання пакетів SMB із сервером. Якщо замість цього встановлено значення вимкнено, клієнт взагалі не намагатиметься узгоджувати підписання пакетів SMB.

Microsoft більше не рекомендує використовувати параметри «якщо згоден сервер» або «якщо згоден клієнт», оскільки ці параметри впливають тільки на SMB версії 1, необхідно відключити, бо вона також є застарілою та додає тільки додаткові вразливості. Відключається SMB першої версії за допомогою PowerShell скріпту, який запускається на усіх робочих станціях за допомогою доменного серверу AD.

2.3 Усунення загроз що реалізуються зі сторони користувача

Окрім загроз які реалізуються завдяки потрапляння зловмисника у внутрішню мережу офісу, де знаходиться робоча станція оператора, такими ж небезпечними та можливо ймовірнішими є атаки які порозводяться за допомогою

неосвіченості користувача або атаки які навмисно зі злим наміром проводить сам користувач робочої станції:

- Витік інформації з вкраденого носія інформації;
- Витік інформації за допомогою шкідливого ПЗ, яке користувач запускає на робочій станції (навмисно чи через свою необачність);
- Витік інформації за допомогою зовнішнього носія інформації (персонального носія з умислом вкрасти інформацію чи шкідливого носія, який користувач вирішив під'єднати до робочої станції);
- Доступ до локального облікового запису Windows завдяки зовнішнього носія з ПЗ для розгортання ОС Windows.

2.3.1 Усунення загрози витіку інформації з вкраденого носія інформації

Для того щоб запобігти витоку інформації з внутрішнього носія інформації робочої станції поперед усе треба запобігти крадіжці самого носія інформації. У даному випадку станція знаходиться під цілодобовим відео наглядом охорони, усі системні блоки робочих станцій запломбовано та щоб їх відкрити знадобляться інструменти та деякий час – тобто усім робітникам та охороні буде легко помітити особу яка намагається дістати жорсткий диск із корпусу робочої станції та запобігти цьому.

Але вищеназвані заходи упираються в обізнаність та чесність працівників офісу, що не є надійним. Тому додатково необхідно впровадити шифрування внутрішнього носія інформації робочої станції, яке не дасть зловмиснику получити доступ до інформації робочої станції, навіть якщо він якимось чином зможе отримати сам внутрішній носій інформації робочої станції.

У нашому випадку це необхідно зробити для ОС Windows. ОС передбачає таку можливість за допомогою функції повного шифрування BitLocker, яка вбудована у ОС Windows починаючи з Windows Vista. BitLocker призначений для захисту даних, забезпечуючи шифрування для цілих розділів жорсткого диску. За замовчуванням він використовує AES із 128-бітним або 256-бітним ключем, тобто є досі надійним так як при надійному паролі для брутфорсу такого диску знадобяться десятиріччя.

Для увімкнення шифрування за допомогою BitLocker треба просто увімкнути цю функцію у ОС. У нашому випадку це треба зробити для усіх 400 робочих станцій, тому це потрібно автоматизувати.

Це також можна зробити за допомогою управління груповими політиками на контролері домену. Для цього попередньо необхідно встановити відповідний модуль на контролер домену через додання ролей та особливостей домену.

Після того як відповідний модуль інстальовано, можна буде створити групові політики, які відповідають за шифрування носіїв інформації робочих станцій та знаходяться по шляху Конфігурація комп'ютера > Адміністративні шаблони > Компоненти Windows > Шифрування диска BitLocker.

Тут присутній достатньо великий перелік групових політик для налаштування шифрування під різні вимоги, наприклад можна вимагати PIN та додаткову аутентифікацію кожного разу, коли запускається робоча станція або дозволяти доступ до носія тільки при наявності зовнішнього USB-носія з відповідним ключем для дешифрування.

Буде застосовано наступні політики:

- Застосовувати тип шифрування диска на дисках операційної системи – тут можна вибрати буде шифруватися увесь диск, або тільки зайнятий простір. Для оптимальної швидкодії робочої станції необхідно вибрати шифрування тільки зайнятого простіру;
- Зберігати інформацію для відновлення BitLocker у доменних службах Active Directory - Цей параметр політики використовується для налаштування зберігання інформації про відновлення BitLocker в AD DS. Це забезпечує адміністративний метод відновлення даних, зашифрованих BitLocker, щоб запобігти втраті даних через відсутність ключової інформації. Тобто ключ буде зберігатися на контролері домену для аварійного відновлення інформації на зашифрованих носіях;
- Дозволити розблокування диску за допомогою мережі під час запуску – ця політика дозволяє розблокування внутрішнього зашифрованого носія, якій під'єднаний до довіреного контролера домену, за допомогою ключа який

зберігається на контролері домену. При цьому між доменом та робочою станцією встановлюється зашифроване з'єднання, тобто вкрасти ключ прослуховуючи мережу не вийде.

Увімкнення самого шифрування через інструменти групових політик не передбачене, але це можна зробити за допомогою скріпту, який у свою чергу через політику планувальника завдань можна запустити на усіх комп'ютерах у домені. Як можна бачити на рисунку 2.3 Після застосування політик диск буде відображатися зашифрованим. При застосованій конфігурації диск буде автоматично дешифровано на робочій станції без втручання оператора, але при спробі доступі до нього на іншому комп'ютері, не приєднаному до домену він вимагатиме ключа для розблокування – рисунок 2.4. Тобто зловмисник навіть викравши внутрішній накопичувач не зможе получити доступ до інформації, яка на ньому зберігається.

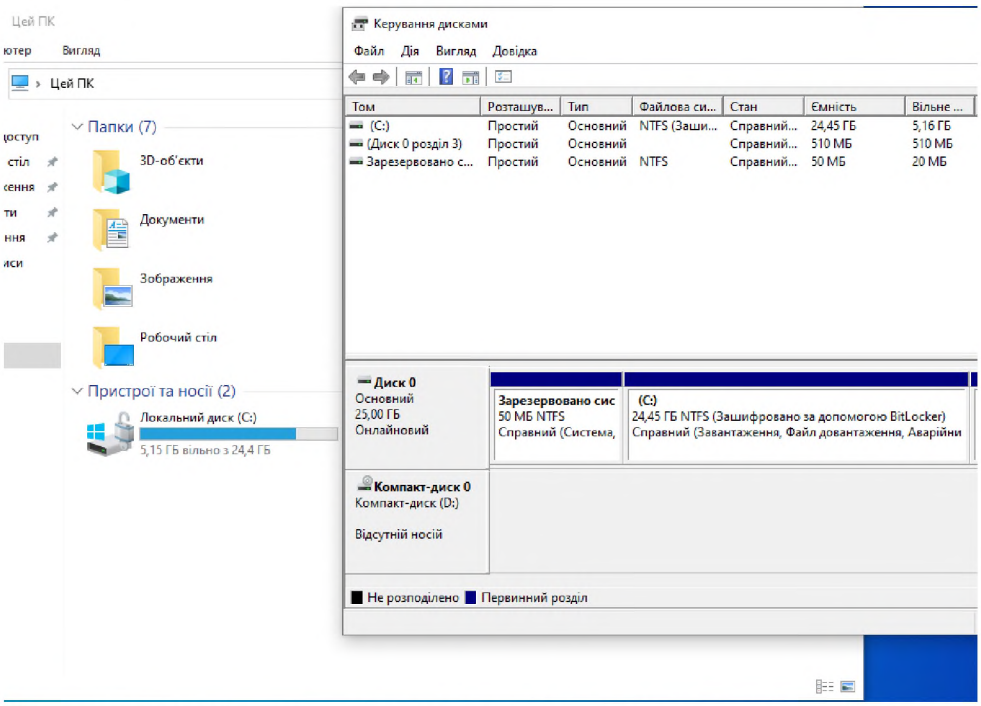


Рисунок 2.3 Приклад того як виглядає диск у системі після шифрування BitLocker

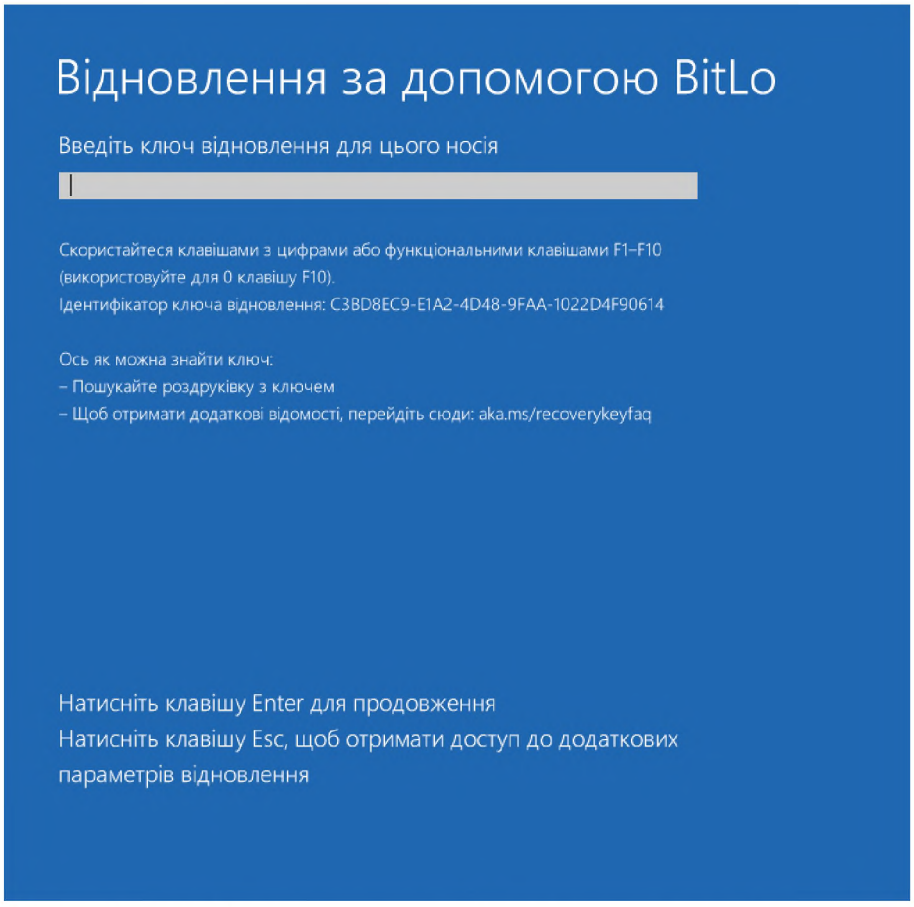


Рисунок 2.4 Як виглядає спроба доступу до змісту зашифрованого диску з іншого

2.3.2 Усунення загрози витоку інформації через шкідливе ПЗ

Один з найрозповсюджених способів атаки – це атака через шкідливе ПЗ. Політики які управляють правилами запуску ПЗ на комп'ютері знаходяться за шляхом Конфігурація комп'ютера > Параметри Windows > Параметри безпеки > Політики обмежень програмного забезпечення. У поточній конфігурації буде найкращім рішенням дозволяти користувачу робочої станції запускати тільки встановлене ПЗ, яке присутнє одразу після розгортання образу, або встановлюється з серверу AD. Також операторами у роботі використовується ПЗ, яке неможливо заздалегідь встановити, так як воно встановлюється тільки для одного облікового запису ОС, тобто кожному користувачу необхідно буде самостійно інсталювати таке ПЗ у своєму обліковому запису. Однак простого рішення тут немає, тому що немає політики яка дозволить запускати тільки вже установлене ПЗ. Рішенням буде заборонити запуск ПЗ з усіх директорій користувача для доступу до яких йому не потребуються адміністративні привілеї

та дозволити запуск з директорій де знаходиться вже установлене ПЗ. ПЗ яке користувачу необхідно буде самостійно інсталювати буде розміщене у загальній папці робочого столу та для з неї буде дозволено запускати ПЗ – так користувач буде бачити установники на своєму робочому столі, зможе їх запустити та інсталювати необхідне ПЗ, але не зможе нічого добавити до суспільного робочого столу, так як для цього необхідні адміністративні привілеї.

Як можна бачити на рисунку 2.5 будуть використовуватися наступні налаштування.

Заборона на запуск ПЗ:

Суспільні директорії:

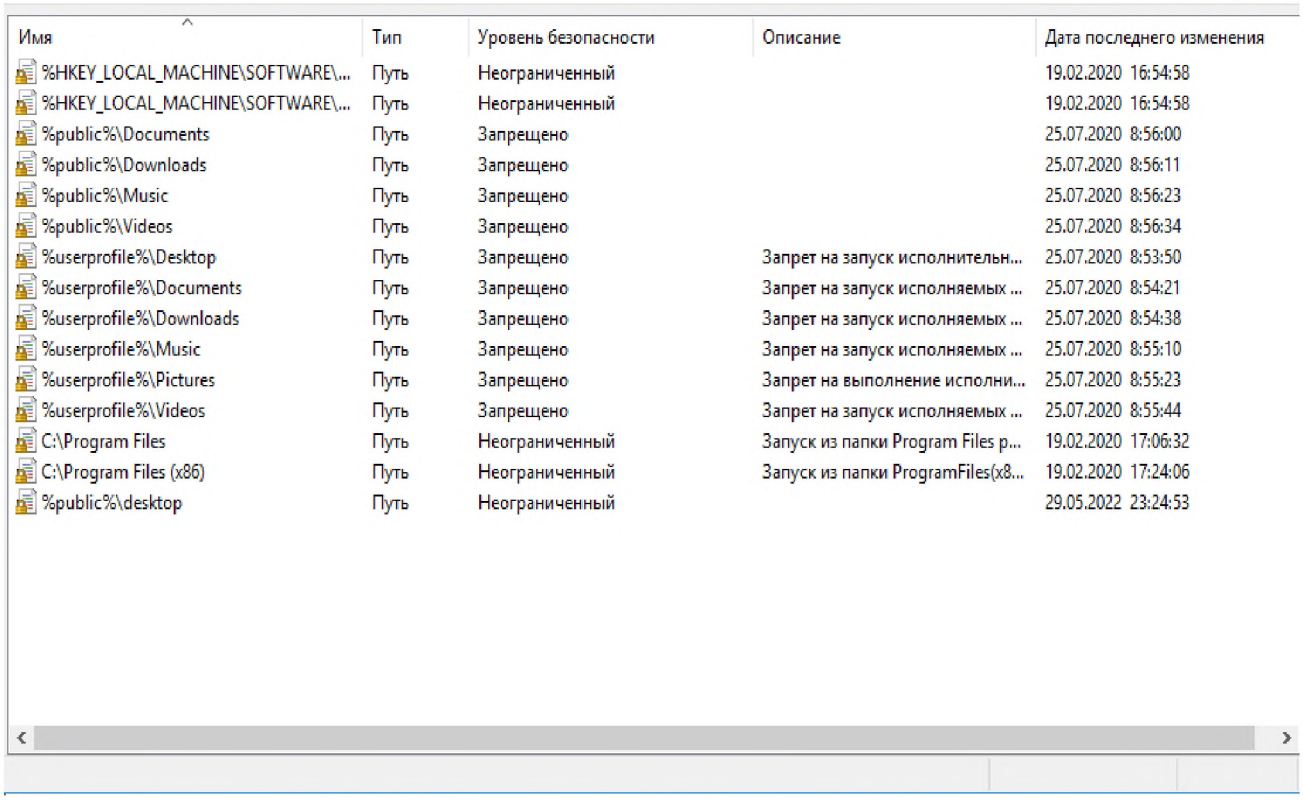
- %public%\Documents –директорія документів;
- %public%\Downloads – директорія завантажень;
- %public%\Music – директорія аудіо-файлів;
- %public%\Videos – директорія відео-файлів.

Персональні директорії кожного окремого користувача робочої станції:

- %userprofile%\Desktop –директорія яка зберігає файли робочого стола;
- %userprofile%\Documents - директорія документів;
- %userprofile%\Downloads – директорія куди потрапляють всі завантаження;
- %userprofile%\Music – директорія аудіо-файлів;
- %userprofile%\Pictures – директорія файлів зображень;
- %userprofile%\Videos – директорія відео-файлів.

Дозвіл на запуск ПЗ:

- C:\Program Files – директорія у якій знаходиться інстальоване ПЗ для 64-розрядних систем;
- C:\Program Files (x86) - директорія у якій знаходиться інстальоване ПЗ для 32-розрядних систем;
- %public%\Desktop – суспільна директорія робочого столу.



Имя	Тип	Уровень безопасности	Описание	Дата последнего изменения
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Путь	Неограниченный		19.02.2020 16:54:58
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Путь	Неограниченный		19.02.2020 16:54:58
%public%\Documents	Путь	Запрещено		25.07.2020 8:56:00
%public%\Downloads	Путь	Запрещено		25.07.2020 8:56:11
%public%\Music	Путь	Запрещено		25.07.2020 8:56:23
%public%\Videos	Путь	Запрещено		25.07.2020 8:56:34
%userprofile%\Desktop	Путь	Запрещено	Запрет на запуск исполнительн...	25.07.2020 8:53:50
%userprofile%\Documents	Путь	Запрещено	Запрет на запуск исполняемых ...	25.07.2020 8:54:21
%userprofile%\Downloads	Путь	Запрещено	Запрет на запуск исполняемых ...	25.07.2020 8:54:38
%userprofile%\Music	Путь	Запрещено	Запрет на запуск исполняемых ...	25.07.2020 8:55:10
%userprofile%\Pictures	Путь	Запрещено	Запрет на выполнение исполни...	25.07.2020 8:55:23
%userprofile%\Videos	Путь	Запрещено	Запрет на запуск исполняемых ...	25.07.2020 8:55:44
C:\Program Files	Путь	Неограниченный	Запуск из папки Program Files р...	19.02.2020 17:06:32
C:\Program Files (x86)	Путь	Неограниченный	Запуск из папки ProgramFiles(x8...	19.02.2020 17:24:06
%public%\desktop	Путь	Неограниченный		29.05.2022 23:24:53

Рисунок 2.5 Налаштування групової політики для заборони запуску програм

При такому налаштуванні користувач не зможе запускати будь-яке ПЗ, якщо воно не було вже заздалегідь встановлене, або попередньо розташовано у суспільній директорії робочого столу.

2.3.3 Усунення загрози витоку інформації за допомогою зовнішнього носія інформації

Крім випадкового витоку інформації, користувач також може навмисно зі злим наміром та для особистою вигоди спробувати вкрасти інформацію з якою він працюю за допомогою зовнішнього носія інформації.

Цьому також можна перешкодити застосувавши групову політику, яка відповідає за взаємодію ОС Windows з зовнішніми носіями. Політика знаходиться по шляху Конфігурація комп’ютера > Політики > Адміністративні шаблони > Система > Доступ до знімного сховища.

Як можна побачити на рисунку 2.6 тут є декілька варіантів як змусити Windows працювати з зовнішніми носіями інформації:

- Заблокувати окремо тільки зчитування інформації з зовнішнього носія;

- Заблокувати окремо тільки запис інформації на зовнішній носій;
- Заблокувати окремо тільки запуск ПЗ з зовнішнього носія;
- Заблокувати будь-яку взаємодію з зовнішніми носіями.

Ці правила можна окремо впроваджувати для різних типів зовнішніх носіїв:

- CD, DVD диски;
- Дискети;
- Стрічкові накопичувачі;
- WPD девайси (медіа плеєри, камери, мобільні телефони та інші);
- Користувацькі класи носіїв інформації за допомогою GUID девайсу.

Останній тип девайсів (користувацькі класи носіїв інформації за допомогою GUID девайсу) дає нам можливість у той же час дозволити використання окремого конкретного носія інформації за допомогою його унікального ідентифікатора – GUID. Це необхідно для зручності системного адміністратора, якому буде потрібно налаштовувати або встановлювати ПЗ вручну.

Для зручності користувача ми можемо обмежити тільки запис та запуск програм з зовнішнього носія інформації, запобігши будь-якому витоку інформації за допомогою зовнішнього носія, та залишив можливість переглядати його зміст. У нашому випадку це не необхідному, тому для даної конфігурації буде вимкнена будь яка взаємодія з зовнішніми носіям у межах ОС. Після застосування політики, як видно на рисунку 2.7 , ОС буде відмовляти в будь -якому доступу до зовнішніх накопичувачів.

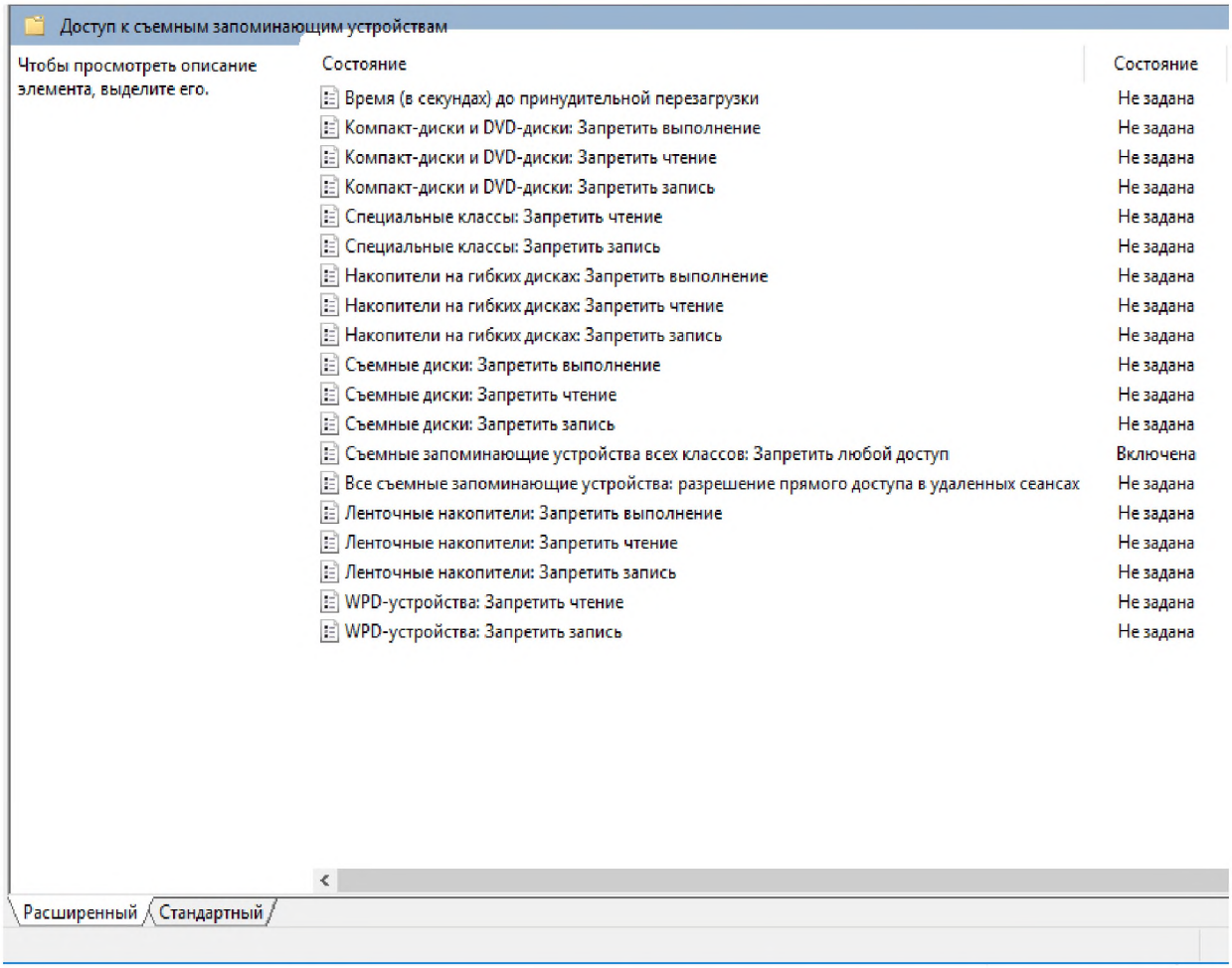


Рисунок 2.6 Налаштування групової політики стосовно зовнішніх накопичувачів

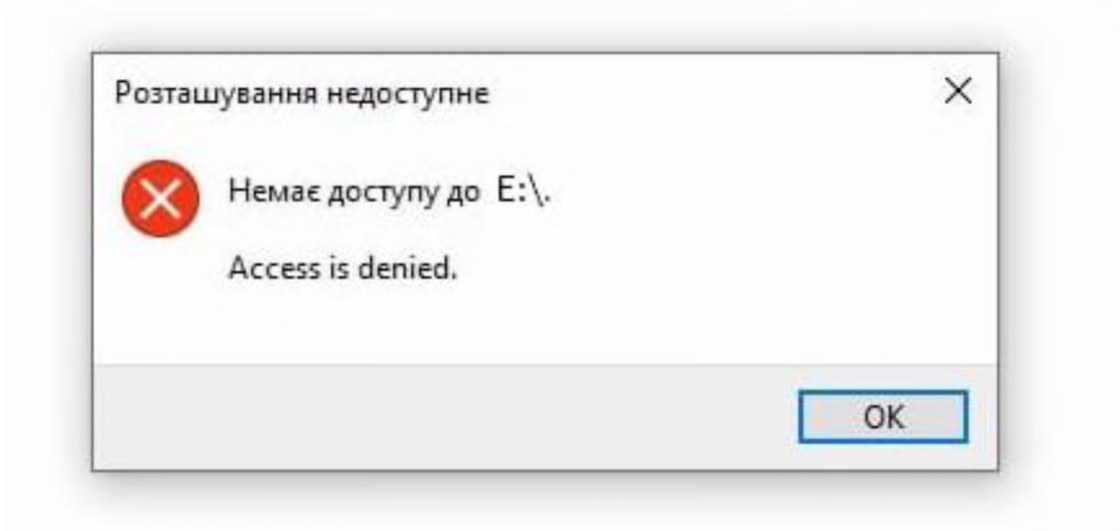


Рисунок 2.7 Приклад того як виглядає спроба взаємодії з зовнішніми носіями після застосування політик

2.3.4 Усунення загрози через злам локального облікового запису

У ОС Windows передбачення досі зручна функція скидання паролю локального облікового запису (у томі числі и облікового запису з адміністративними привілеями) просто за допомогою інсталяційного носія Windows. Це дуже корисно та зручно у разі якщо користувач персонального комп'ютера забув свій пароль. Але у випадку коли комп'ютер потрапив у руки зловмисники а також у нашому випадку це є серйозною вразливістю яка дає можливість необмеженого доступу до даних та ПЗ робочої станції будь-кому з таким носієм (який не складає ніяких труднощів створити) та фізичним доступом до цієї робочої станції. Після зміни зловмисником паролю локального облікового запису, або якщо зловмисник його дізнався за допомогою соціальної інженерії це також у подальшому створює можливість безперешкодного віддаленого підключення до робочої станції через вбудований у ОС Windows протокол RDP, що дає зловмиснику можливість у прямому ефірі спостерігати за оператором який працює з даними клієнта, включаючи паспортні дані та дані про транзакції клієнта. Це усугубляється тим що при здійсненні віддаленого підключення Windows ніяк не повідомляє користувача кінцевого клієнта.

З таким зламом локального облікового запису можна боротися двома путями – це встановити пароль адміністратора у BIOS кожного окремого комп'ютера (а у даному офісі знаходиться більше 400 машин) та відключення будь-яких локальних облікових записів.

Встановлення паролю на BIOS само собою не є трудомістким завданням, але перевірити наявність паролю адміністратора BIOS та встановити його, якщо він відсутній, необхідно на кожній з 400 робочих станцій вручну, бо цей процес не є можливим автоматизувати.

З іншого боку – відключення локальних облікових записів можливо зробити за допомогою групових політик, тобто, як і у попередніх випадка, достатньо запровадити це правило один раз на контролері домену, та усі машини що входять до цього домену автоматично застосують це правило.

Політика знаходиться по шляху: Конфігурація комп'ютера > Політики > Параметри Windows > Параметри безпеки > Локальні політики > Параметри безпеки, та при застосуванні вимикає усі локальні облікові записи с адміністративними привілеями. Тобто навіть якщо зловмисник буде знати пароль локального адміністративного запису, він нічого не зможе зробити. Але обов'язковою умовою для того щоб це працювало, є те що ім'я та пароль адміністративного облікового запису контролера домена (який працює на усіх робочих станціях під'єднаних до нього) має відрізнятися від локального.

2.4 Висновок до другого розділу

У розділі було розглянуто загрози витоку інформації через вразливості робочої станції зі сторони програмного забезпечення та дій користувача, а саме вразливість мережевих протоколів ОС, виток інформації через запуск шкідливого ПЗ, виток інформації завдяки використанню зовнішнього носія інформації, виток інформації з вкраденого внутрішнього носія інформації та можливість зламу локального облікового запису.

Було запропоновано до впровадження методи усунення названих загроз, які реалізуються завдяки вбудованих у ОС групових політик, що дозволяє масово застосувати заходи на усіх робочих станціях через контролер домену.

3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Постановка задачі

У економічному розділу необхідно буде визначити техніко-економічне обґрунтування(ТЕО) - економічну ефективність впровадження описаних у другому розділі заходів інформаційної безпеки.

Мета написання техніко-економічного обґрунтування це зробити фінансову оцінку передбачуваних економічних витрат на впровадження методів інформаційної безпеки, корисний результат завдяки їх впровадженню та їх співвідношення.

ТЕО має містити:

- стислий опис і значення проблеми, яка розглядається у кваліфікаційній роботі;
- обґрунтування необхідності та актуальності вирішення проблеми;
- аналіз очікуваних результати що впровадження програмних І технічних засобів забезпечення інформаційної безпеки;
- сутність запропонованого у кваліфікаційній роботі методу вирішення даної проблеми.

Для проведення техніко-технічного обґрунтування необхідно:

1) Розрахувати капітальні витрати на придбання та налагодження ПЗ та апаратних складових системи інформаційної безпеки які необхідні для впровадження методів описаних у другій частині;
2) Розрахувати річні експлуатаційні витрати на утримання і обслуговування ПЗ та апаратних складових;
3) Визначити річний економічний ефект від впровадження обраних заходів;
4) Визначити та проаналізувати показники економічної ефективності впроваджених заходів;
5) Зробити висновок про економічну доцільність впроваджених заходів.

3.2 Виконання розрахунків

3.2.1 Розрахунок капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

До капітальних інвестицій відносяться витрати на впровадження обраних заходів збереження безпеки інформації при роботі оператора на робочій станції. Це визначається виходячи з трудомісткості впровадження обраних заходів.

Трудомісткість реалізації впровадження заходів визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного з спеціалістів інформаційної безпеки).

$$t = tmз + tв + ta + tозб + tp + tд \qquad (3.1)$$

де ttз - тривалість складання технічного завдання на пошук та усунення загроз безпеки інформації;

tв - тривалість аналізу ТЗ, вивчення інформації щодо можливих вразливостей безпеки інформації та їх пошуку;

ta – тривалість аналізу присутніх у поточній конфігурації вразливостей та їх реалізації;

tвз - тривалість визначення вимог до заходів, методів та засобів захисту;

tозб - тривалість вибору основних рішень з забезпечення безпеки інформації;

tвпр - тривалість впровадження обраних заходів;

tд - тривалість документального оформлення політики безпеки.

Для обраних заходів наведені величини становлять: ttз = 24 години, tв = 72 години, ta = 40 годин, tвз = 32 години, tозб = 24 години, tвпр = 80 годин, tд = 24 години.

Відповідно,

t = 24+72+40+32+24+80+24 = 296 годин

Розрахунок витрат на розробку та впровадження заходів.

Витрати на розробку політики безпеки інформації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації Змч:

$$Крп = Ззп + Змч \quad (3.2)$$

Заробітна плата виконавця/виконавців враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, тощо) і визначається за формулою:

Ззп = t*Зпр = 296*139.4 = 41262.4 грн (3.3)

де t – загальна тривалість розробки політики безпеки, годин;

Зпр – середньогодинна заробітна плата інженера комп'ютерних систем з нарахуваннями, грн/година.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

Змч = t·Смч , грн, (3.4)

де t - трудомісткість розробки політики безпеки інформації на ПК, годин;

Смч - вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = Р * tнал * Се + \frac{Фзал + На}{F} + \frac{Клпз + Напз}{F}, грн \quad (3.5)$$

де Р - встановлена потужність ПК, кВт;

Се - тариф на електричну енергію, грн/кВт·година;

ФЗал - залишкова вартість ПК на поточний рік, грн.;

На - річна норма амортизації на ПК, частки одиниці;

Нат - річна норма амортизації на ліцензійне програмне забезпечення, частки одиниц1;

Клт - вартість ліцензійного програмного забезпечення, грн.;

Fр - річний фонд робочого часу (за 40-годинного робочого тижня Fр = 1920).

У цьому випадку:

Р = 0.055 кВт;

Се = 1,68 грн/кВт*година

ФЗал = 14500 грн

На = 0,125

Клт = 0 (використовується безкоштовне ПЗ)

Fр = 1920

$$\text{Смч} = 0.055 * 296 * 1.68 + \frac{14500 * 0.125}{1920} = 28.29 \text{ грн}$$

Крп = 41262.4 + 28.29 = 41290.69 грн

Капітальні (фіксовані) витрати на проектування та впровадження заходів для усунення вразливостей інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} \quad (3.6)$$

де Кпр - вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

Кзпз - вартість закупівлі ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

Крп - вартість розробки політики безпеки інформації, тис. грн;

Каз - вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

Кнавч - витрати на навчання технічних фахівців і обслуговуючого персоналу, тис.грн;

Кн - витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

Кпр = 400 тис. грн (повторний пентест мережі)

Кзпз = 0 (усе необхідне ліцензійне ПЗ вже присутнє)

Каз = 0 (усе необхідне обладнання вже присутнє)

Кнавч = 60 тис. грн (витрати на навчання та підвищення кваліфікації інженера комп'ютерних систем стосовно роботи з AD та перевірки мережі на вразлиовсті)

Кн = 0 (витрати на впровадження заходів вже входять у розраховане Крп)

К = 400 + 60 + 41 = 501 тис. грн

3.2.2 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати - це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

До поточних (експлуатаційних) варто відносити наступі витрати:
вартість Upgrade-відновлення й модернізації системи (Св);
витрати на керування системою в цілому (Ск);
витрати, викликані активністю користувачів системи інформаційної безпеки (Сак - "активність користувача").

Під "витратами на керування системою" маються на увазі витрати, пов'язані з керуванням і адмініструванням серверів та інших компонентів системи інформаційної безпеки. До цієї статті витрат можна віднести наступні витрати:

- навчання адміністративного персоналу й кінцевих користувачів;
- амортизаційні відрахування від вартості обладнання та ПЗ;
- заробітна плата обслуговуючого персоналу;
- аутсорсинг (тобто залучення сторонніх організацій для виконання
- деяких видів обслуговування);
- навчальні курси й сертифікація обслуговуючого персоналу;
- технічне й організаційне адміністрування й сервіс.

Для цієї ситуації витрати за рік будуть складати:

Св = 8000 грн (витрати на змінні частини та обслуговування серверного обладнання, згідно з останнім роком)

Ск буде складатися з заробітної плати інженера, його навчання

Сзп = 139.4 грн/год * 1994 год = 277963.6 грн - заробітної плати інженера

Снав = 100 000 грн – щорічний бюджет на навчання інженера

Ск = 377963.6 грн

Сак часткова входить до Ск, так як прямою допомогою та додатковим налаштуванням також займається інженер комп’ютерних систем, тож Сак буде

складатися з витрат на навчання операторів, тобто заробітної плати тренеру, що проводить навчання

Сак = 120.75 грн/год * 1994 год = 240775.5 грн

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

С = Св + Ск + Сак (3.7)

С = 8000 + 377963.6 + 240775.5 = 626739.1 грн

3.3 Визначення річного економічного ефекту:

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки 1 становить:

E= B·R-C (3.8)

де В - загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R - очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

С - щорічні витрати на експлуатац1ю системи інформаційної безпеки, тис грн.

У даному випадку атака на робочу станцію не перешкоджає роботі оператора, не приводить до простою чи втраті інформації, та взагалі може довгий час пройти непоміченою. Збиток буде представляти з себе адміністративну відповідальність у виді штрафу від 500 до 1000 неоподатковуваних мінімумів доходів громадян [12]. Для розрахунків візьмемо 2 суми штрафу через те що втеча даних може відбуватись більш одного разу на рік.

В = 2 * 1240.5 * 1000 = 2481000 грн

Е = 2481000 *0.8 – 618 638 = 1358060.9 грн

3.4 Визначення та аналіз показників економічної ефективності

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи:

$$ROSI = \frac{E}{K}, \text{частки одиниці} \qquad (3.9)$$

де Е – загальний ефект від реалізації захисних методів, грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI дорівнює:

$$ROSI = \frac{1358060}{618\,638} = 2.19$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (Nрдс - Nінф) / 100 \qquad (3.10)$$

Де Nрдс – річна депозитна ставка (15%);

Nінф – річний рівень інфляції (10.9%)

2.19 > (15 – 10.9)/100 ~ 2.19 > 0.041

Термін окупності капітальних інвестицій То показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від реалізації впровадження обраних заходів безпеки інформації:

$$To = \frac{К}{Е} = \frac{1}{ROSI}, \text{ років} \qquad (3.11)$$

$$To = \frac{1}{2.19} = 0.46 \text{ року}$$

3.4 Висновок третього розділу

При проведені техніко-технічного обґрунтування було визначено, що розмір капітальних витрат на впровадження заходів ліквідації вразливостей безпеки інформації зі сторони робочої станції оператора складає 501 тис грн, річні поточні витрати на функціонування системи скла-дають 626739 грн.

Впровадження обраних заходів є економічно доцільним, оскільки коефіцієнт повернення інвестицій складає 2.19 грн до грн, що означає отримання 2.19 грн економічного ефекту на кожну гривню капітальних вкладень задля усунення описаних вразливостей, при цьому термін окупності буде складати 0,46 року ~ 168 днів.

ВИСНОВОК

У роботі було проаналізовано вбудовані вразливості зі сторони робочої станції під керуванням ОС Windows. Їх усунення є актуальним питанням, через те що цією операційною системою користується 80% користувачів у світі, при цьому для реалізації цих загроз не потрібні додаткові навички чи поглибленні знання принципу роботи мережі чи вразливостей за допомогою яких вони реалізуються.

Проаналізовані вразливості є небезпечними для звичайного користувача, та особливо небезпечними для комерційного сектору, через те що вони можуть призвести до витоку чутливої інформації, яка зберігається на персональному комп'ютері. Рівень небезпечності цих загроз також підтверджується нещодавніми найкрупнішими атаками, які призвели до дуже великих втрат та майже зупинці цілого комерційного сектора – WannaCry та NotPetya.

В роботі запропоновано методи запобігання витоку інформації зі сторони робочої станції:

- від атак через шкідливе ПЗ;
- від витоку інформації за допомогою зовнішніх носіїв інформації;
- від витоку інформації з внутрішнього носія інформації робочої станції;
- від вразливостей через некоректне налаштування програмного забезпечення робочої станції.

В економічному розділі розраховані необхідні витрати на розробку названих заходів та економічна доцільність їх впровадження.

ПЕРЕЛІК ПОСИЛАНЬ

1 What is WannaCry ransomware? URL: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

2 The Untold Story of NotPetya, the Most Devastating Cyberattack in History (ANDY GREENBERG) URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

3 How often do Cyber Attacks occur? URL: https://aag-it.com/how-often-do-cyber-attacks-occur/

4. Використання ОС у всьому світі URL: https://gs.statcounter.com/os-market-share

5. Документація ПЗ Responder URL: https://github.com/SpiderLabs/Responder

6. Документація OS Kali URL: https://www.kali.org/docs/

7. Документація ПЗ ОС Kali URL: https://www.kali.org/tools/

8. Документація ПЗ Wireshark URL: https://www.wireshark.org/docs/

9. Документація ОС Ubuntu URL: https://help.ubuntu.com

10. Протоколи ОС Windows URL: https://docs.microsoft.com/en-us/openspecs/protocols/ms-protocolslp/9a3ae8a2-02e5-4d05-874a-b3551405d8f9

11. Документація використання групових політик AD URL: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831791(v=ws.11)

12. Захист персональних даних у Україні https://patriot.legal/ru/zahyst-personalnyh-danyh-v-ukrayini/

13. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук - Дніпро: НТУ «ДП», 2020. - 47 с.

14. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека/ Упорядн.: Д.П. Пілова. - Дніпро: Національний технічний університет "Дніпровська політехніка", 2019. - 16 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	1	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі.	18	
6	А4	Спеціальна частина.	16	
7	А4	Економічний розділ	6	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	

ДОДАТОК Б. Перелік документів на оптичному носії
Залевский_МВ_125_18_1_ПЗ.docx
Залевский_МВ_125_18_1_ПЗ.pdf
Залевский_МВ_125_18_1_ДМ.pptx
Залевский_МВ_125_18_1_ПЗ.pdf.p7s

ДОДАТОК В. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу бакалавра студента групи 125-18-1
Залевського Максима Владиславовича
на тему «Підсистема захисту інформації робочої станції оператора колцентра банківської установи».

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 58 сторінках.

Метою кваліфікаційної роботи є розробка підсистеми захисту інформації робочої станції колцентра банківської установи..

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека», а зміст та структура роботи дозволяють розкрити поставлену тему повністю.

Для досягнення поставленої мети в кваліфікаційній роботі вирішуються задачі виявлення вразливостей у налаштуванні робочих станцій, аналізу загроз що через них реалізуються та пропонуються методи для їх усунення.

Практична цінність полягає у розробці рекомендацій щодо створення підсистеми захисту робочої станції колцентра банківської установи.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів

В ході виконання кваліфікаційної роботи студент Залевський М.В. проявив самостійність та показав добрий рівень володіння теоретичними положеннями з обраної теми та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки « 80 / Добре ».

Керівник кваліфікаційної роботи

к.т.н., доц каф БІТ Герасіна О.В.

Керівник спец. розділу

асистент кафедри БІТ Ю.А. Мілінчук

Відгук керівника кваліфікаційної роботи

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 85 б. («Добре»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)