**Лабораторна робота №2.**

**Тема:** ” Інструментальні засоби захисту, firewall ”

**Мета роботи:** ознайомитись з основними видами firewall’ів, принципами їх роботи, ефективністю, можливостями.

**Короткі теоретичні відомості**

Брандмауер - це не просто маршрутизатор, хост або група систем, які забезпечують безпеку в мережі, швидше, брандмауер - це підхід до безпеки; він допомагає реалізувати політику безпеки, яка визначає дозволені служби і типи доступу до них, і є реалізацією цієї політики в термінах мережевої конфігурації, декількох хостов і маршрутизаторів, і інших заходів захисту, таких як посилена аутентифікація замість статичних паролів. Основна мета системи брандмауера - управління доступом До або З мережі, що захищається. Він реалізує політику мережевого доступу, примушуючи проходити усі з'єднання з мережею через брандмауер, де вони можуть бути проаналізовані і дозволені або знехтувані.

Система брандмауера може бути маршрутизатором, персональним комп'ютером, хостом, або групою хостів, створеною спеціально для захисту мережі або підмережі від неправильного використання протоколів і служб хостами, що знаходяться поза цією підмережею. Зазвичай система брандмауера створюється на основі маршрутизаторів верхнього рівня, зазвичай на тих, які сполучають мережу з Інтернетом, хоча може бути створена і на інших маршрутизаторах, для захисту тільки частини хостов або підмереж.

Компоненти брандмауера, основними компонентами брандмауера є:

- політика мережевого доступу

- механізми посиленої аутентифікації

- фільтрація пакетів

- прикладні шлюзи

**Хід роботи**

В результаті виконання було надано розширений доступ до папки на машині 1. Результат спільного доступу зображено на рисунку 2.1.

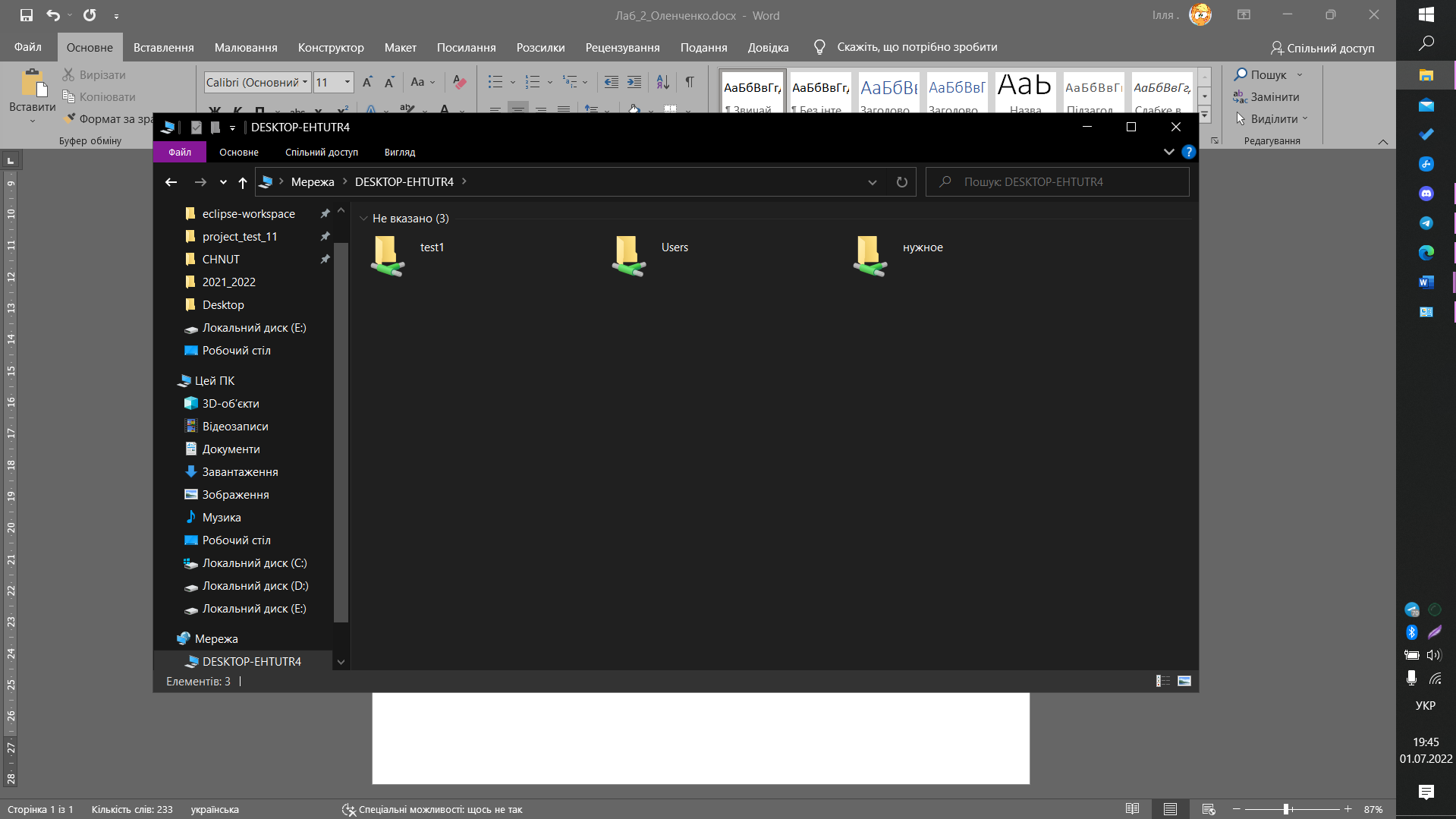


Рисунок 2.1 - Доступ до папки test1 з машини 2

Результат зміни політики брендмауера - виключено спільний доступ до папок та принтерів, зображено на рисунку 2.2.

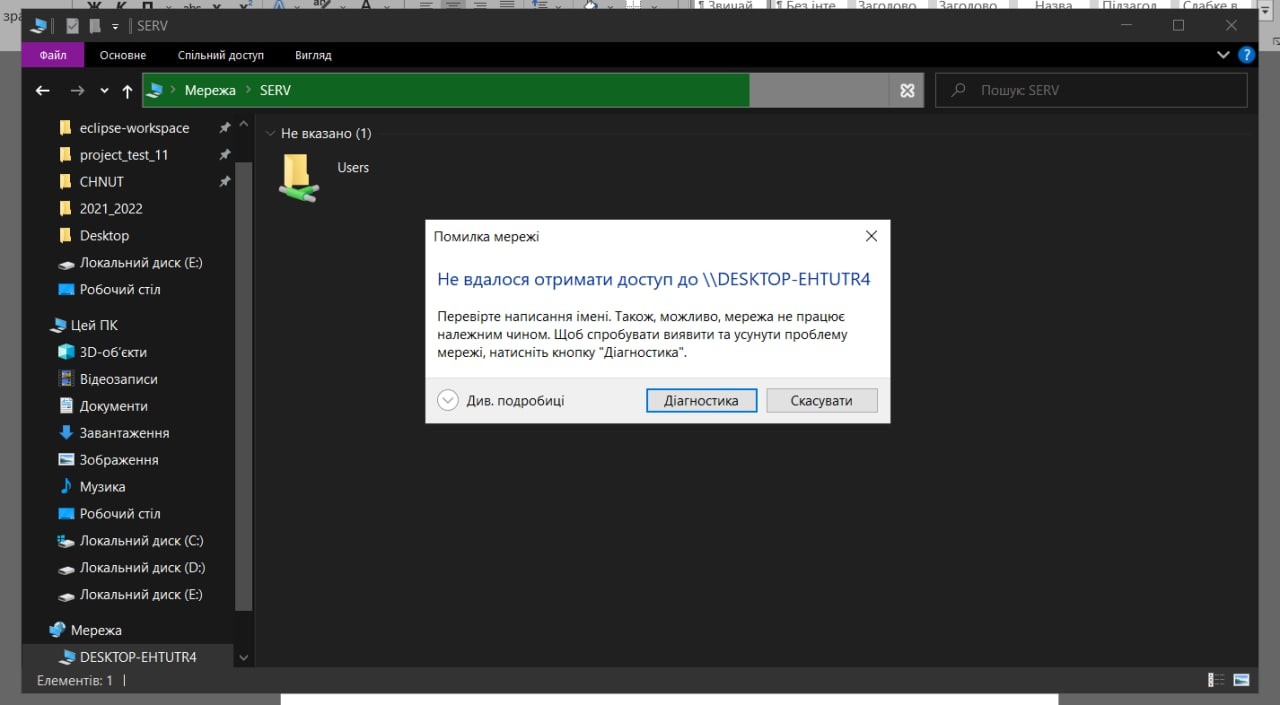


Рисунок 2.2 - Втрата доступу до папки

Короткі імена доступних служб зображені на рисунку 2.3.

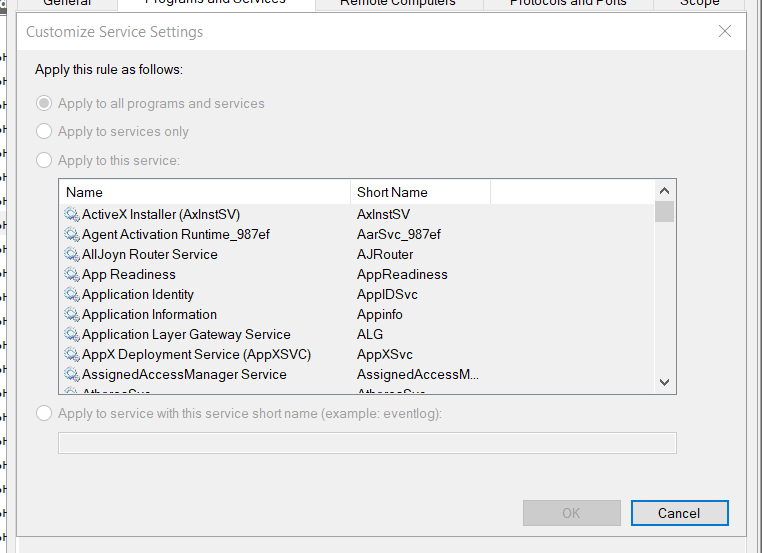


Рисунок 2.3 - Короткі імена служб

Доступні та вибрані типи ICMP зображені на рисунку 2.4.

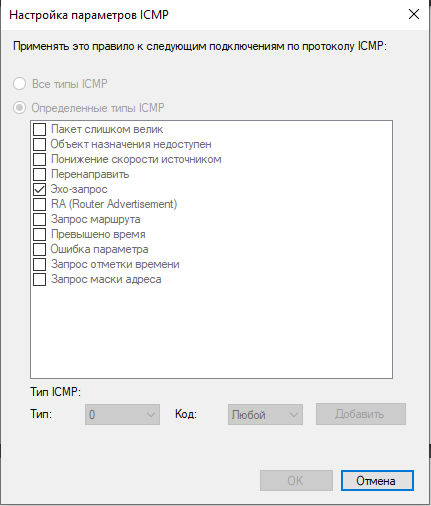


Рисунок 2.4 - Типи ICMP

Для досліджень було вибрано брандмауер TinyWall.

TinyWall здійснює аналіз мережевої активності комп'ютера, «переглядає» відкриті порти та регулює доступ встановлених програм до мережі Інтернет, звіряючись із заданими всередині програми правилами.

Брандмауер працює за принципом "заборонити все, що не дозволено". Це означає, що програма заблокує доступ до мережі для всіх програм, служб та портів, за винятком тих, що внесені до так званого «білого списку». При цьому файрвол надає користувачеві кілька режимів роботи: звичайний (рекомендований), при якому TinyWall працюватиме згідно з довірчим списком, як описано вище; режим часткового та повного блокування. Згідно порядку часткового блокування програма надасть можливість вихідних з'єднань за допомогою LAN-підключення деяким компонентам операційної системи. У разі застосування правил повної заборони доступу буде відмовлено їм усім.

Для недопущення зміни правил зловмисниками TinyWall надає користувачам можливість парольного захисту. Ця опція особливо актуальна у випадках поперемінного використання одного комп'ютера кількома людьми.

Головні плюси даного брандмауера:

- використовує мало пам'яті, що робить хорошим вибором для систем з невеликим обсягом оперативної пам'яті;

- безкоштовно, без реклами та без спливаючих вікон;

- Підтримує магазин Windows. Автоматично виявляє та обробляє всі пакети UWP;

- Фільтри TinyWall активні від початку після завантаження ОС.

Мінуси:

- Не відкритий вихідний код

- Під час блокування програм фаєрвол не показує сповіщення.

Результати тестування брандмауерів сканером безпеки зображено в таблиці 2.1.

Таблиця 2.1 - Результати тестування

|  |  |  |  |
| --- | --- | --- | --- |
| Загроза | Без брандмауера | Вбудований в ОС | TinyWall |
| Руткіт: MissingDriverLoad | Захищений | Захищений | Захищений |
| Руткіт: LoadAndCallImage | Захищений | Захищений | Захищений |
| Руткіт: DriverSupersede | Захищений | Захищений | Захищений |
| Руткіт: ChangeDrvPath | Вразливість | Вразливість | Вразливість |
| Вторгнення: Runner | Захищений | Захищений | Захищений |
| Вторгнення: RawDisk | Вразливість | Вразливість | Вразливість |
| Вторгнення: PhysicalMemory | Захищений | Захищений | Захищений |
| Вторгнення: FileDrop | Вразливість | Вразливість | Вразливість |
| Вторгнення: DebugControl | Захищений | Захищений | Захищений |
| Ін’єкція: SetWinEventHook | Вразливість | Вразливість | Вразливість |
| Ін’єкція: SetWindowsHookEx | Вразливість | Вразливість | Вразливість |
| Ін’єкція: SetThreadContext | Захищений | Захищений | Захищений |
| Ін’єкція: Services | Вразливість | Вразливість | Вразливість |
| Ін’єкція: ProcessInject | Захищений | Захищений | Захищений |
| Ін’єкція: KnownDlls | Захищений | Захищений | Захищений |
| Ін’єкція: CreateRemoteThread | Захищений | Захищений | Захищений |
| Ін’єкція: APC dll injection | Захищений | Захищений | Захищений |
| Ін’єкція: AdvancedProcessTermination | Захищений | Захищений | Захищений |
| ICMP Test | Захищений | Захищений | Захищений |
| DNS Test | Вразливість | Вразливість | Захищений |
| Підміна особи: OLE automation | Захищений | Захищений | Захищений |
| Підміна особи: ExplorerAsParent | Захищений | Захищений | Захищений |
| Підміна особи: DDE | Вразливість | Вразливість | Захищений |
| Підміна особи: Coat | Вразливість | Вразливість | Вразливість |
| Підміна особи: BITS | Захищений | Захищений | Захищений |
| Викрадання: WinlogonNotify | Захищений | Захищений | Захищений |
| Викрадання: Userinit | Захищений | Захищений | Захищений |
| Викрадання: UIHost | Захищений | Захищений | Захищений |
| Викрадання: SupersedeServiceDll | Вразливість | Вразливість | Вразливість |
| Викрадання: StartupPrograms | Вразливість | Вразливість | Вразливість |
| Викрадання: ChangeDebuggerPath | Вразливість | Вразливість | Вразливість |
| Викрадання: AppinitDlls | Вразливість | Вразливість | Вразливість |
| Викрадання: ActiveDesktop | Захищений | Захищений | Захищений |

При виконанні тестування утилітою ping до системи з увімкненим брандмауером, брандмауер приймає вхідні запити але не відповідає. Результат зображено в журналі пакетів wireshark на рисунку 2.5. При розгортанні серверу FTP, брандмауер також буде виконувати ігнорування запитів на під’єднання. Також виконується блокування DNS запитів через утиліту nslookup, зображено на рисунку 2.7.

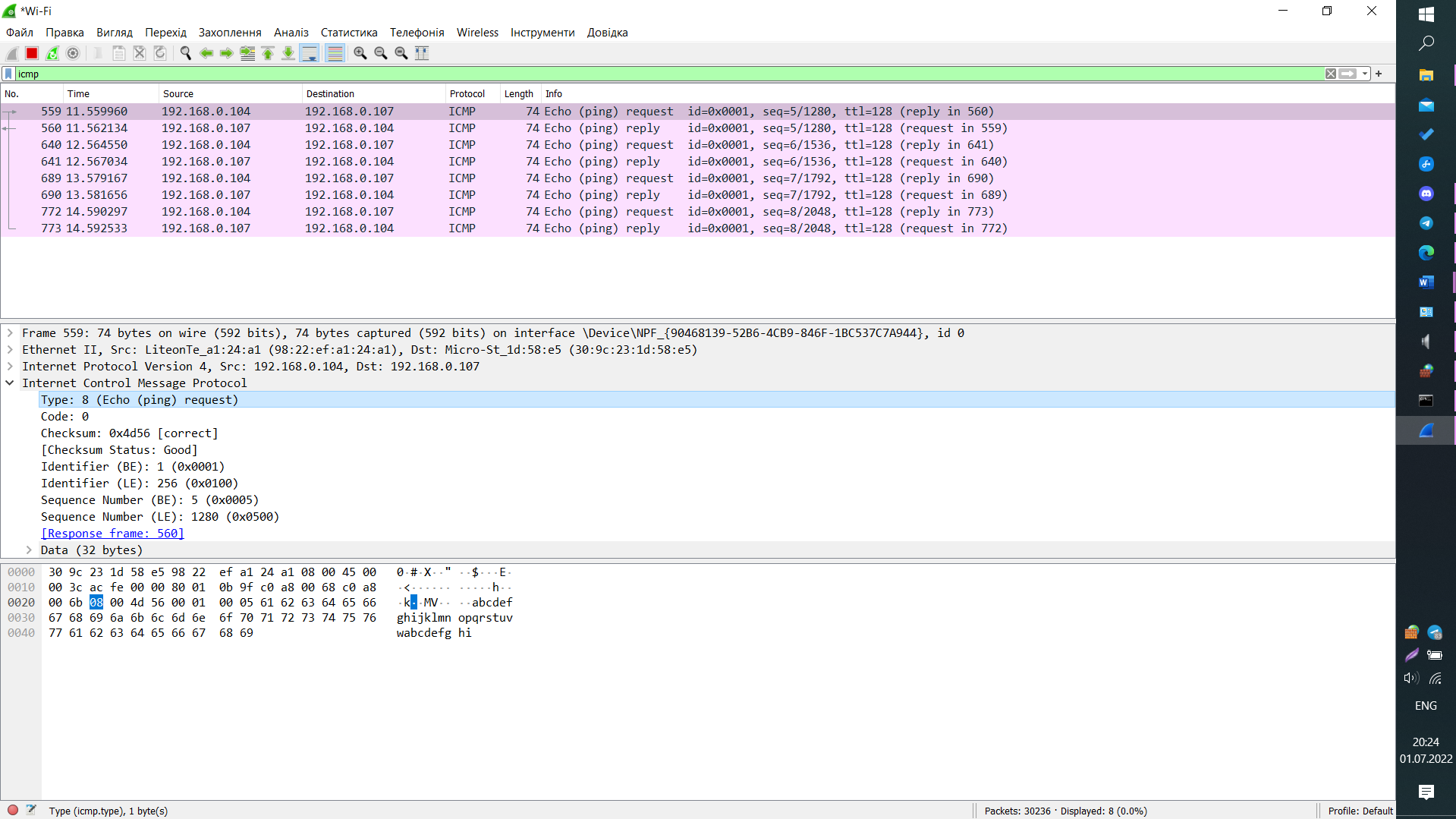


Рисунок 2.5 - Фільтрація пакетів ICMP

З’єднання що були заблоковані брандмауером зображені на рисунку 2.7

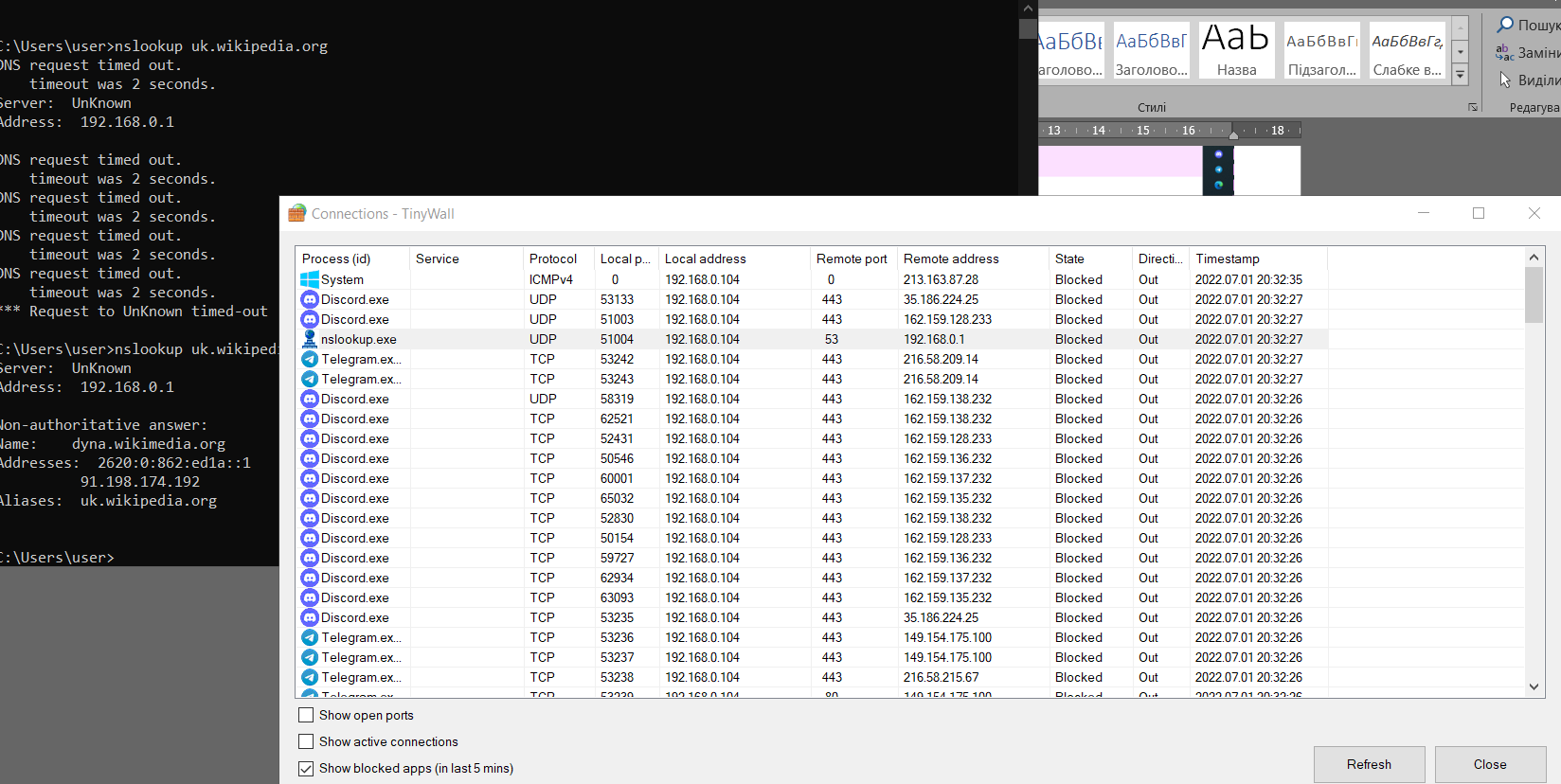


Рисунок 2.7 - Заблоковані з’єднання

Висновок: на даній лабораторній роботі я ознайомивсь з основними видами фаерволів, принципами їх роботи, ефективністю та можливостями. Виконав встановлення кастомного брандмауера та виконав тестування його роботи.