МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Комп'ютерна інженерія»

Група: 2БКС-26

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

здобувача освіти денної форми навчання

БКС.26.20.000.КРБ

ШЕВЧУКА МАРКА СЕРГІЙОВИЧ

м. Одеса
2022 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: **«Комп'ютерна інженерія»**

Група: **2БКС-26**

ПОЯСНЮВАЛЬНА ЗАПИСКА

До кваліфікаційної роботи бакалавра на тему:_____

«Розробка мережевого фільтру на базі одноплатного міні комп'ютера RASPBERRY PI»

Проектний матеріал складається з пояснювальної записки на _____ сторінках та графічного (презентаційного) матеріалу на _____ аркушах (слайдах)

Виконавець _____ (Шевчук М.С)

Керівник проекту_____ (Іванова Л.В.)

Консультанти:

з охорони праці_____ (Чорновол Н.І.)

з дотримання вимог ЄСКД _____ (Петрашова В.І.)

старший консультант _____ (Скорнякова О.В.)

До захисту допущений

Завідувачка кафедри _____ (Іванова Л.В.)

Завідувач відділення _____ (Суліма Ю.Ю.)

Захист «____»_____ 202____ р. Протокол ДКК №_____

Оцінка ЕК _____

Секретар ДКК _____

АНОТАЦІЯ

Тема дипломної роботи «Розробка мережевого фільтру на базі одноплатного міні комп’ютера RASPBERRY PI».

У цій роботі описаний принцип розробки мережевого фільтру використовуючи pi hole .

У аналітичній частині приведене технічне завдання до проекту, а також принцип роботи мережевих протоколів. В технологічній частині приведені інструменти для розробки мережевого фільтру та порівняння з аналогами. У розділі реалізація представлена покрокова інструкція реалізації мережевого фільтра з використанням безкоштовних інструментів, таких як pi hole та pi vpn. Останнім розділом стала охорона праці під час розробки та конструювання додатку.

Ключові слова: Ad block , raspberry pi , розробка, Pi hole , Pi vpn , DNS фільтр, Raspbian, Windows.

ANNOTATION

Thesis topic "Development of a network filter based on a single-board mini computer RASPBERRY PI".This paper describes the principle of developing a network filter using pi hole.

In the analytical part the technical task to the project, and also the principle of work of network protocols is resulted. In the technological part the tools for development of the network filter and comparison with analogues are resulted. The implementation section provides step-by-step instructions for implementing a network filter using free tools such as pi hole and pi vpn. The last section was labor protection during the development and design of the application.

Keywords: Ad block, raspberry pi, development, Pi hole, Pi vpn, DNS filter, Raspbian, Windows.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *комп'ютерних систем* Кафедра *комп'ютерної інженерії*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР ***Беркань І.В.***

"_____" _____202____р.

З А В Д А Н Н Я

на кваліфікаційну роботу бакалавра

Шевчук Марк Сергійович

Здобувачеві (здобувачці) освіти

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи

Розробка мережевого фільтру на базі одноплатного міні комп'ютера RASPBERRY PI

затверджена наказом по коледжу від "____"_____202____р. №_____

2. Термін здачі кваліфікаційної роботи____20.06.2022р.

3. Вихідні дані до роботи

1. Вимоги щодо запровадження мережевих фільтрів

2. Функціональні вимоги щодо мережних фільтрів

3. Апаратні вимоги до мережевої архітектури

4. Програмні вимоги до мережевої архітектури

5. Вимоги мережної безпеки

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Вступ . Аналітичний огляд мережних технологій для реалізації мережних фільтрів. Визначення технічного завдання на роботу. Реалізація мережевого фільтру. Тестування мережевого фільтру. Розділ охорони праці Висновок. Перелік використаних джерел інформації.

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

1. Структурна схема мережевого фільтру

2. Функціональна схема мережевого фільтру

3. Алгоритм роботи мережевого фільтру

4. Алгоритм налаштування мережевого фільтру

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів роботи, що стосується їх

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Основний	*Іванова Л.В.*	*30.11.2021*	*17.05.2022*
Охорона праці	*Чорновол В.І.*	*4.05.2022*	*17.05.2022*
Нормоконтроль	*Петрашова В.І.*	*4.05.2022*	*17.05.2022*
Старший консультант	*Скорнякова О.В.*	*4.05.2022*	*17.05.2022*

7. Дата видачі завдання *30.11.2021*

Керівник роботи *Іванова Л.В.*
(підпис)

Завдання прийняв до виконання *Шевчук М.С.*
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	*Передмова*	*4.05.2022*	
2.	*Аналітичний огляд мережних технологій для реалізації*	*8.05.2022*	
	мережних фільтрів	*10.05.2022*	
3.	*Визначення технічного завдання на роботу*		
4.	*Реалізація мережевого фільтру*	*15.05.2022*	
5.	*Тестування мережевого фільтру*	*17.05.2022*	
6.	*Розділ охорони праці*	*22.05.2022*	
7.	*Висновок*		
8.	*Перелік літератури*	*26.05.2022*	
9.	*Оформлення пояснювальної записки*	*28.05.2022*	
10.	*Оформлення графічної частини*	*31.05.2022*	
11.	*Малий захист кваліфікаційної роботи*	*2.06.2022*	
12.	*Захист кваліфікаційної роботи*	*15.06.2022*	
		18.06.2022	

Виконавець *Шевчук М.С.*
(підпис)

Керівник роботи *Іванова Л.В.*
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 26.20.000.00 КР	Кваліфікаційна робота		
А4			БКС 26.20.000.00 КР ПЗ	Пояснювальна записка	1	
			БКС 26.20.000.00 КР МП	Мультимедійна презентація		

Ізм.	Арк.	№ докум.	Підпис	Дата	БКС 26.20.000.00 БКР ПЗ		
Розробив		Шевчук М.С.			Розробка мережевого фільтру на базі одноплатного міні комп'ютера RASPBERRY PI	Літ.	Аркуш 3 / Аркушів 51
Перевірив		Іванова Л.В.				Н Д П	
Н. Контр.		Петрашова В.				ВСП «ОТФК ОНТУ» гр.БКС-26	
Затверд.		Скорнякова О.					

ЗМІСТ

ПЕРЕДМОВА

Використання інтернету є невід'ємною частиною нашого життя. Ми можемо в ньому проводити по години або по пів дня використовуючи різні ресурси, такі як перегляд відео на youtube, фільмів або серіалів на rezka або просто перегляд стрічки в instagram.

Мережевий трафік, який завантажується містить не тільки бажану інформацію, але так само і не потрібну інформацію у вигляді реклами. Ця реклама може бути у вигляді дрібного посту в стрічці або дрібним банером в кутку форуму, але як частіше буває це хвилинна або три хвилинна реклама у відео яке триває менше хвилини або величезний банер на весь екран який не можна закрити через відсутність оптимізації браузера смартфона, або як це частіше буває переадресація на нову вкладку з рекламним сайтом після закриття якого вас чекатиме хвилинна реклама на самому відео. Комбінацій може бути безліч, а рішення тільки одне - закрити сайт та знайти інший. Але що , якщо ви дивитеся ваш улюблений серіал або новини на вашому дорогому смарт TV, який ви купували не для перегляду реклами, виникає необхідність вирішення таких проблем.

Можна запропонувати два способи вирішити цю проблему: оплачувати місячну передплату улюбленому хостингу або виконати ряд нескладних дій і забезпечити себе та свою сім'ю мережевим фільтром, який усуне всю набридливу та нетактовну інформацію від очей ваших дітей, учнів та інших глядачів.

Звичайно мережевий фільтр потрібен не тільки для домашнього використання, він є невід'ємною частиною навчального закладу. Адже в самій рекламі можуть бути присутні посилання на неприйнятний контент для учнів та здобувачів освіти навчальних закладів. Так само, якщо користувач не досвідчений він може нашкодити персональному комп'ютеру, встановлюючи програмне забезпечення з рекламних посилань, які можу завдати шкоди по цифровій інформації або відкрити доступ до віддаленого входу і вкрасти

цифрові ліцензійні ключі від платних навчальних програм.

Інформація вище також стосується співробітників різних корпорацій або дрібних бізнесів. Скільки можна було б заощадити ресурсів компаній як у співробітників не повністю обмежений доступ до інтернету, а обмежений доступ до реклами.

Як далі буде показано мережевий фільтр може не тільки блокувати рекламу, але і доступ до різних хостингів це допоможе з навчанням ваших дітей без відрізання їх від інтернету, а також підвищить працездатність співробітників і дасть їм доступ до мережі з вже обмеженими ресурсами.

Pi-hole не буде редагувати ваш трафік він працює в таким спосібом. Коли ви хочете переглянути сайт, скажімо, **www.baddomain.com** через HTTP або HTTPS, ваш браузер повинен знати, як знайти **www.baddomain.com**, тому він надсилає DNS-запит з питанням «Де я можу знайти цей сайт?» Оскільки все в Інтернеті йде за фактичною IP-адресою, вам необхідно знати IP-адресу, на якій знаходиться цей домен. DNS-запит (те, що вимагає **www.baddomain.com** і переводить це в IP-адресу) йде до Pi-hole та перевіряє, чи є цей домен, який слід відвідати, чи його слід заблокувати. Якщо відвідування дозволено, IP-адреса домену передається назад у браузер, потім браузер відвідує цю IP-адресу і запитує вміст веб-сервера, який відправляється назад або HTTP, або HTTPS. Якщо це домен, який має бути заблокований, IP-адреса, яка відправляється назад, належить самій Pi-hole, і натомість ви отримуєте вміст заблокованої сторінки. Ви навіть не отримаєте вміст поганого домену.

РОЗДІЛ 1. АНАЛІТИЧНИЙ ОГЛЯД ІСНУЮЧИХ РІШЕНЬ

1.1 Огляд технологій мережевого фільтру

Мережевий веб-фільтр — це рішення для інтернет-фільтрації, яке захищає всю мережу від веб-загроз, на відміну від рішень для інтернет-фільтрації, які передбачають встановлення клієнтів на кожен окремий пристрій, підключений до мережі. Його перевага полягає в можливості захистити всю мережу з одного єдиного порталу адміністрування, навіть якщо мережа надає послуги для кількох місць.

Мережевий веб-фільтр не тільки захищає мережу від веб-загроз, але й дозволяє мережевим адміністраторам застосовувати політики допустимого використання для мережних користувачів. Залежно від гнучкості рішення мережеві адміністратори повинні мати можливість застосовувати різні допустимі політики використання для окремих користувачів, груп користувачів та всієї мережі.

1.2 Перспективи використання мережевого фільтру

Основною перевагою мережевих веб-фільтрів є підвищений захист від шкідливих програм, програм-вимагачів та фішингових атак. Якщо мережа заражена шкідливим ПЗ, в результаті програми-здирника відбувається втрата даних або фінансові втрати через успішно проведену фішингову атаку, наслідки можуть бути руйнівними. Багато невеликих організацій були змушені закритися після цих подій.

Інші переваги включають підвищення продуктивності на робочому місці, запобігання проблемам з персоналом і, коли мережа Wi-Fi є загальнодоступною, більш безпечне середовище перегляду для клієнтів, гостей та відвідувачів.

Звіти про історію веб-активності можуть використовуватися підприємствами індустрії гостинності для створення маркетингових акцій, адаптованих до інтересів їхніх клієнтів, а рішення для мережевої фільтрації можуть допомогти підприємствам у регульованих галузях дотримуватися

законодавства про конфіденційність та безпеку. Окрім того, реалізація мережевого веб-фільтра може претендувати на отримання школами грантів та знижок E-rate.

1.3 Основні мережеві протоколи

Мережевий фільтр використовує TCP протокол для створення мережевого підключення між пристроями.

Transmission Control Protocol - TCP є популярним протоколом зв'язку, використовуваним зв'язку через мережу. Він поділяє будь-яке повідомлення на серії пакетів, які відправляються від джерела до призначення, і там воно збирається на місці призначення. Якщо один пакет буде пошкоджений або не дійде, він буде постійно запитуватися у джерела поки не пройде.

Інтернет-протокол - IP розроблений спеціально як протокол адресації. Він переважно використовується з TCP. IP-адреси в пакетах допомагають маршрутизувати їх через різні вузли в мережі, доки вони не досягнуть системи призначення.

У цій роботі я відмовився від використання мережевого протоколу UDP принцип його роботи полягає в тому що він без переривчасто відправляє інформацію на хост не помічаючи того що частина пакетів вже втрачені.

Протокол користувальницьких дейтаграм UDP - це протокол зв'язку, що замінює протокол управління передачею, реалізований в першу чергу для створення зв'язку між різними програмами, що допускає втрати і малої затримки. Ці втрати можуть бути кретичними принцип роботи цього протоколу можна побачити на кабельному Tv.

Отримати доступ до мережевого фільтру можна за допомогою монітора і клавіатури або використовуючи мережевий інтерфейс. Підключиться до мережевого інтерфейсу можна за допомогою Putty або через браузер. Використовуючи мережевий протокол HTTPS можна отримати захищений видалений доступ

Безпечний протокол передачі гіпертексту HTTPS - це стандартний протокол захисту зв'язку між двома комп'ютерами, один з яких використовує браузер, а інший - отримання даних з веб-сервера. HTTP використовується для передачі даних між клієнтським браузером (запит) та веб-сервером (відповідь) у гіпертекстовому форматі, те саме у випадку HTTPS, за винятком того, що передача даних виконується в зашифрованому форматі. Таким чином можна сказати, що https заважає хакерам інтерпретувати або змінювати дані під час передачі пакетів.

1.4 Види мережевих фільтрів

Веб-фільтрація – це запобігання доступу співробітників, студентів та інших кінцевих користувачів до контенту в Інтернеті. Найчастіше блокується контент, який є образливим, неприйнятним чи небезпечним.

Вбудовані веб-фільтри

Вбудовані веб-фільтри – це програмні або апаратні пристрої, які працюють у мережі, яку вони фільтрують. Ці рішення встановлюються як шлюз, який безпосередньо перехоплює весь трафік через мережу.

Оскільки вони не вимагають встановлення програмного клієнта на кожній кінцевій точці, вони часто використовуються в середовищі з гостьовими мережами, пристроями на змішаних платформах або в інших обставинах, коли прямий контроль за пристроями неможливий.

DNS-фільтрація

З точки зору кінцевого користувача, блокування веб-сайтів за допомогою фільтра системи доменних імен аналогічне веб-фільтрації з використанням URL-фільтра. Обидва рішення дозволяють внести веб-сайт до чорного списку програмного забезпечення веб-фільтрації, щоб запобігти доступу до веб-сайту.

Основні відмінності:

Фільтрування DNS не може блокувати доступ до веб-сайтів на основі URL-адреси; натомість він блокує цілі домени.

Веб-фільтр URL діє безпосередньо на трафік TCP / HTTPS, а фільтрація

DNS впливає на вихідні DNS-запити, які передують спробам підключення TCP / HTTPS.

Фільтр DNS вимагає, щоб весь інтернет-трафік перенаправлявся на зовнішній DNS-сервер, що надається постачальником послуг веб-фільтрації.

Фільтрування ключових слів

Веб-фільтрація на основі ключових слів блокує доступ кінцевих користувачів до веб-сайтів, що містять певні ключові слова у текстових рядках. Ці ключові слова ідентифікуються за допомогою регулярних виразів або визначеного списку заблокованих ключових слів.

Метою використання ключових слів для веб-фільтрації є запобігання доступу користувачів до неприйнятного контенту, однак через проблему Скантorпа фільтрація ключових слів може блокувати доступ до законних веб-сайтів. Тому замість цього зазвичай використовуються веб-фільтри на основі категорій, які включають категорії, орієнтовані на дорослих.

Ці бази даних необхідно постійно оновлювати, щоб не відставати від нових веб-сайтів у міру їхнього створення. Тому база даних найчастіше надається постачальником рішень веб-фільтрації.

URL-фільтрація

Якщо ви хочете отримати доступ до певної веб-сторінки, ви повинні ввести уніфікований покажчик ресурсів в адресний рядок , наприклад www.youtube.com/ або www.youtube.com/feed/subscriptions . Фільтрування URL-адрес блокує або дозволяє доступ до певних веб-сайтів або веб-сторінок на основі цих URL-адрес.

Фільтрування URL-адрес забезпечує більш точну та детальну веб-фільтрацію, ніж фільтрація DNS, дозволяючи компаніям блокувати окремі веб-сторінки , а не весь веб-сайт відразу. Щоб спростити блокування цілих веб-сайтів, веб-фільтри на основі URL-адрес можуть також дозволяти фільтрацію за підстановочними знаками , яка блокує весь веб-сайт, якщо винятки не додані до списку дозволених.

Браузерні фільтри

Блокувальники веб-сайтів на основі браузера — це розширення, програми або надбудови, специфічні для кожного окремого браузера. Вони найчастіше використовуються людьми, які хотіли б заблокувати відволікаючі веб-сайти. Ці фільтри рідко використовуються в бізнес-налаштуваннях , оскільки їх легко оминути за допомогою іншого браузера.

Фільтри пошукових систем

Пошукові системи зазвичай використовують будь-який метод фільтрації явних результатів пошуку . Ці веб-фільтри дозволяють використовувати пошукові системи в середовищах, де контент для дорослих вважатиметься недоречним, наприклад, у школах, публічних бібліотеках та більшості робочих місць.

Програмне забезпечення для веб-фільтрації на основі кінцевих точок

Програмне забезпечення веб-фільтрації на основі кінцевих точок має програмний клієнт, який підтримує фільтрацію комп'ютерів або користувачів, що дозволяє настроювати рішення веб-фільтрації для кожного пристрою або студента/співробітника/відвідувача.

Програмні клієнти отримують оновлення політики веб-фільтрації з центрального сервера, яким керує компанія, і зберігають політики, навіть коли пристрої відключаються від мережі.

Брандмауери

Брандмауери - це різновид вбудованих фільтрів веб-контенту. Брандмауери можуть бути апаратними пристроями або віртуальними пристроями на основі хмарних/програмних засобів. Замість того , щоб блокувати певні веб-сайти, брандмауери фільтрують мережевий трафік авторизованими портами, протоколами та IP -адресами.

Традиційні брандмауери з фільтрацією пакетів працюють на рівні 3 (мережевому рівні) моделі OSI для фільтрації портів, протоколів та IP -адрес. Хоча ці типи брандмауерів дійсно блокують веб-трафік, їм не вистачає

1.5 Загрози у мережі Інтернет

На сьогоднішній день відомі такі види мережевих атак:

mailbombing - простий і невигадливий спосіб кібератаки, суть якого полягає у порушенні нормальної роботи електронної пошти адресата шляхом закидання його поштової адреси повідомленнями великого об'єму або у великих кількостях

IP-спуфінг - вид хакерської атаки, що полягає у використанні чужої IP-адреси джерела з метою обману системи безпеки. Метод, який використовується в деяких атаках. Полягає у зміні поля "адреса відправника" IP-пакета.

DDOS-атака - хакерська атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, за яких сумлінні користувачі системи не зможуть отримати доступ до системних ресурсів, що надаються, або цей доступ буде утруднений.

Man-in-the-Middle - вид атаки у криптографії та комп'ютерній безпеці, коли зловмисник таємно ретранслює та за необхідності змінює зв'язок між двома сторонами, які вважають, що вони безпосередньо спілкуються один з одним.

XSS-атака - тип атаки на веб-системи, що полягає у впровадженні сторінку шкідливого коду, що видається веб-системою, і взаємодії цього коду з веб-сервером зловмисника.

Фішинг - вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів - логін та паролів.

1.6 Мережевий фільтр у навчальному закладі

Сьогоднішні здобувачі освіти народжуються в повністю цифровому світі, і викладачі просто не можуть дозволити собі відмовитись від допомоги у розвитку навичок цифрової грамотності, необхідних їм для досягнення успіху. Навчальні заклади відреагували на цей попит, запропонувавши програми, які

надають здобувачам освіти програмне забезпечення, які вони можуть використовувати в навчальному закладі та брати з собою додому.

1.7 Технічне завдання по розробці мережевого фільтру

Мережевий фільтр був створений для контролю мережевого трафіку, не обмежуючи доступ користувачів до корисних загальнодоступних ресурсів, але убезпечивши цей доступ до шкідливих та марних сайтів.

Використовуючи безкоштовні інструменти з відкритим кодом, створити корисний модуль який буде фізично підключений до маршрутизатора і дасть нам можливість впливати на вхідний мережевий трафік.

Під "безкоштовними інструментами" я мав на увазі такі розробки як "PI hole та PI VPN".

Pi - hole - це застосування для реклами на рівні мережі Linux і блокування інтернет-трекерів, яке діє як воронка DNS і, можливо, як DHCP- сервер, призначене для використання в приватній мережі.

Pi VPN - це сервер OpenVPN, розроблений для роботи на Raspberry Pi . Він надає доступ до домашньої мережі через безпечне з'єднання. Підключивши Raspberry Pi до маршрутизатора, він діє як міст між мобільними пристроями і вашою мережею.

Для цієї розробки потрібно придбати raspberry pi. Є варіант з мінімальним внеском купивши raspberry pi zero w , але в цій роботі я використав raspberry pi model 3.

Характеристики для raspberry pi zero w

- Чіп: Broadcom BCM2835 з CPU та GPU
- Процесор CPU: ARM1176JZ-F із тактовою частотою 1 ГГц
- Графічний співпроцесор: VideoCore IV із тактовою частотою 400 МГц
- RAM-пам'ять: Elpida B4432BBPA-10-F 512 МБ
- Бездротовий модуль: CYW43438

- Частотний діапазон: 2,4 ГГц
- Стандарт Wi-Fi: 802.11b/g/n
- Стандарт Bluetooth: BLE v4.1
- Цифровий аудіо/відео вихід: mini-HDMI
- Композитний відеовихід: 2 піна під розпаювання
- Порт для периферії: Micro USB з OTG
- Роз'єм відеокамери: Camera Serial Interface (MIPI CSI)
- Карта пам'яті: MicroSD
- Порти введення-виводу: 40
- Габарити: 66×32×5 мм

Характеристики для raspberry pi model 3

- Однокристальна система: SoC Broadcom BCM2837B0
- Центральний процесор: 4-ядерний 64-бітний CPU на Cortex-A53 (ARMv8) із тактовою частотою 1,4 ГГц
- Графічний процесор: VideoCore IV GPU із тактовою частотою 400 МГц
- Оперативна пам'ять: 512 МБ LPDDR2 SDRAM
- Стандарт Wi-Fi: 802.11.b/g/n/ac (2,4 та 5 ГГц)
- Стандарт Bluetooth: v4.2 із BLE
- Максимальна вихідна роздільна здатність: 1080p (60 Гц)
- Аналоговий аудіо / відеовихід: 4-контактний міні-джек 3,5 мм
- Порт для периферії: USB 2.0
- Порт для екрану: Display Serial Interface (MIPI DSI)
- Карта пам'яті: microSD
- Напруга живлення: 5 В
- Максимальний струм споживання: 2,5 А
- Розміри плати з урахуванням роз'ємів: 67×58×12 мм

РОЗДІЛ 2. РЕАЛІЗАЦІЯ МЕРЕЖЕВОГО ФІЛЬТРУ

2.1 Обґрунтування вибору одноплатного міні комп’ютера

Pi - це одноплатний комп'ютер, а це означає, що мікропроцесор, пам'ять, безпровідні радіомодулі і порти знаходяться на одній друкованій платі. Цього недостатньо для серйозної роботи, але що дійсно робить **Pi** особливим, так це його універсальність.

Програмне забезпечення **Linux** і відкриті контакти введення-виведення загального призначення(GPIO) у верхній частині плати спрощують підключення перемикачів, датчиків і джерел світла, тому любителі можуть дешево прототипировать божевільні ідеї. **Pi** також має аудіороз'єм для навушників або динаміків , порт HDMI для відео, Bluetooth для аксесуарів і підтримку дротяного і безпровідного Інтернету. Він здатний легко переглядати веб-сторінки, обробляти тексти, грати в ретро-игры і запускати різні програми кодування, коли це необхідно.

Для реалізації цього дипломного проекту нижче представлений список **PI** на яких можна буде запустити блокувальник…

Raspberry pi zero w

Цей крихітний недорогий Raspberry Pi має розміри всього 66 x 30,5 x 5 мм і важить всього 9 г. Це не найшвидший Pi - він використовує одноядерний процесор з тактовою частотою 1 ГГц і всього 512 МБ оперативної пам'яті - але його більш ніж достатньо для багатьох задач, особливо тих, що пов'язані камерами.

На відміну від свого дешевшого брата, Raspberry Pi Zero, Zero W має вбудований Wi-Fi 802.11n із Bluetooth 4.0. Тим не менш, Zero W поставляється без підключених контактів GPIO, тільки з отворами для них; вам потрібно буде купити набір контактів та припаяти їх. У цьому Pi також відсутній повнорозмірний USB-порт, замість нього використовується мікро-USB, тому вам може знадобитися якийсь адаптер.

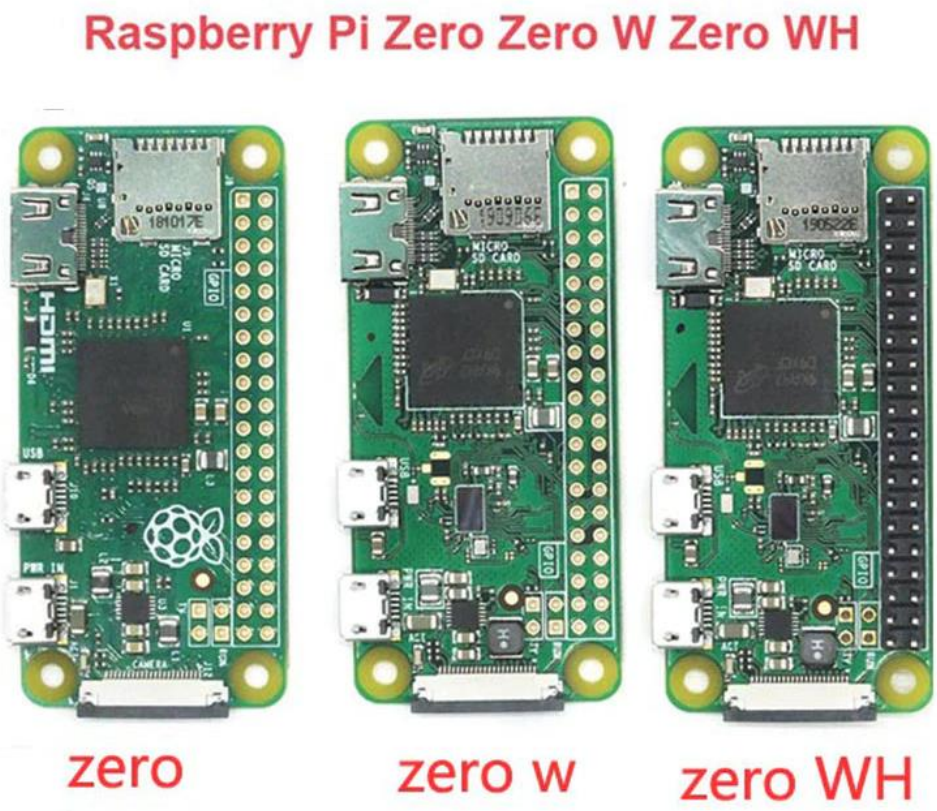

Рис. 2.1 – Raspberry Pi Zero

Raspberry pi 3

Ця модель покоління повільніша, ніж 4 версія, і в них відсутні деякі ключові функції, але з ними працює більше аксесуарів. Вони також використовують стандартні кабелі HDMI і можуть отримувати живлення від багатьох стандартних зарядних пристроїв для телефонів або навіть USB-порту на ПК рекомендується 2,5 A , 5 v , тому у вас, ймовірно, вже є необхідні кабелі.

Raspberry Pi 3 B / 3 B+ також виділяє значно менше тепла, ніж 4 і споживає менше енергії, тому, якщо ви хочете зробити проект, який добре працює, буде пасивне охолодження, і ви можете знайти 3 B / 3 B+ за хорошою ціною, Це хороший вибір. Відмінності між 3B та 3B+ незначні: останній має тактову частоту ЦП на 200 МГц, швидший Ethernet та Wi-Fi 802.11ac (порівняно з 802.11n).

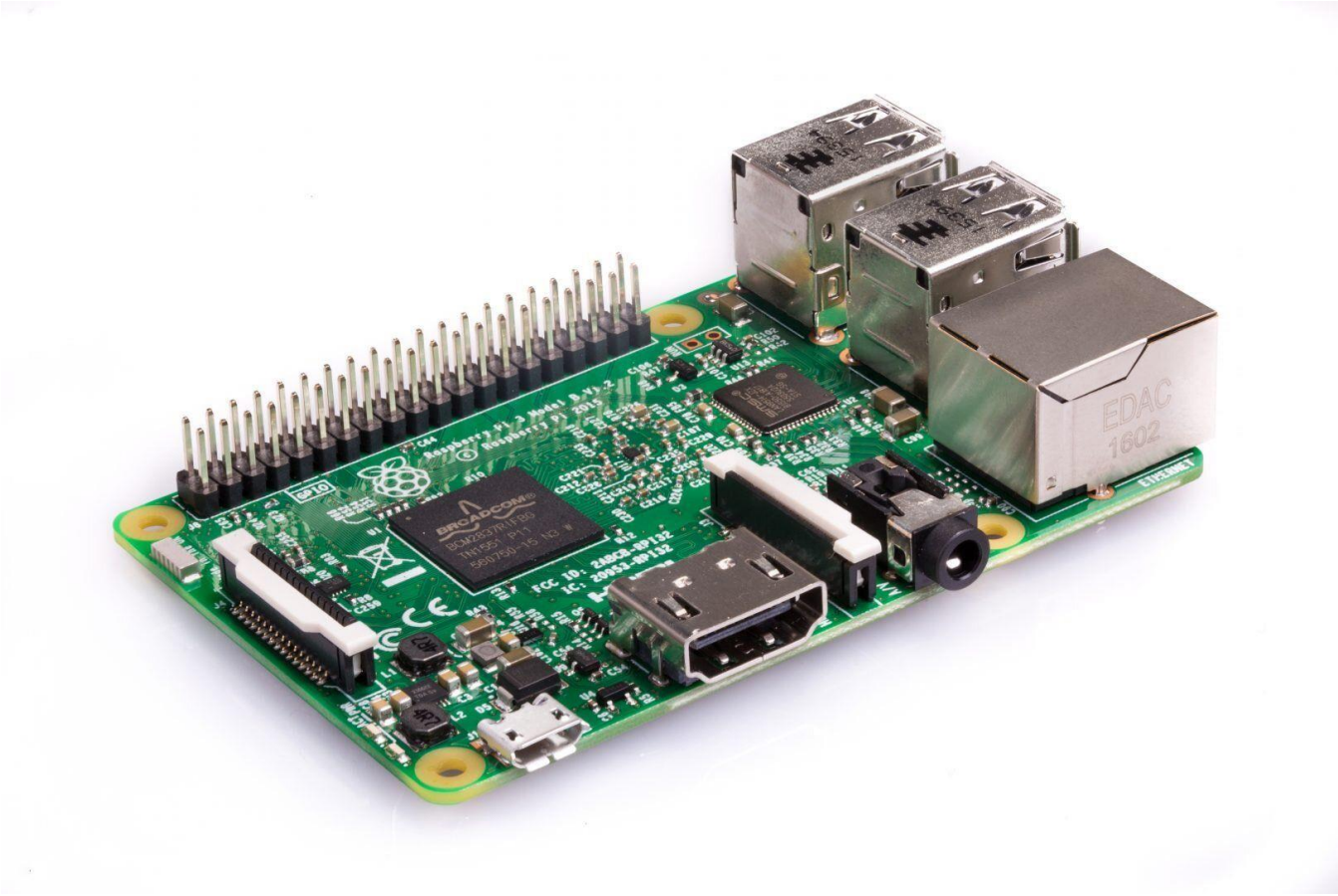

Рис. 2.2 – Raspberry Pi 3

2.2 Підготовка до встановлення raspbian ОС

Перед установкою **raspbian ОС** потрібно підготувати допоміжні інструменти.

Для початку завантажуємо SD Card Formatter, він потрібен для повного форматування SD карти пам'яті для raspberry pi. Цей інструмент безкоштовний і його можна завантажити з офіційного сайту, перейшовши за першим посиланням.

Після півгодинного форматування SD карти завантажуємо наступний інструмент ImageWriter. Ця програма дозволить нам записати raspbian образ на SD карту, що дозволить нам встановити raspbian ОС на основні розділи пам'яті raspberry. Сам ImageWriter безкоштовний та загальнодоступний інструмент, який можна завантажити, перейшовши за першим посиланням.

Та й передостання деталь перед самою установкою. Завантажуємо iso образ із raspbian з офіційного сайту. Там є два формати – перший це light без графічної оболонки, а другий – це вже більш зручний для нас Desktop. Завантажити цей образ можна через офіційний сайт Raspberry pi.

- Відформатував SD Card, використовуючи Overwrite format

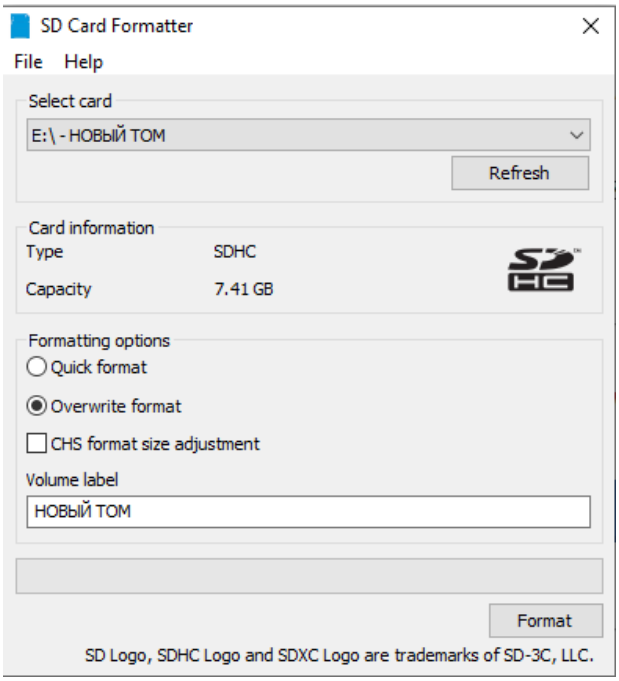

Рис. 2.3 – Інтерфейс SD Card Formatter

- Вибравши iso, raspbian записав на вже відформатовану sd карту

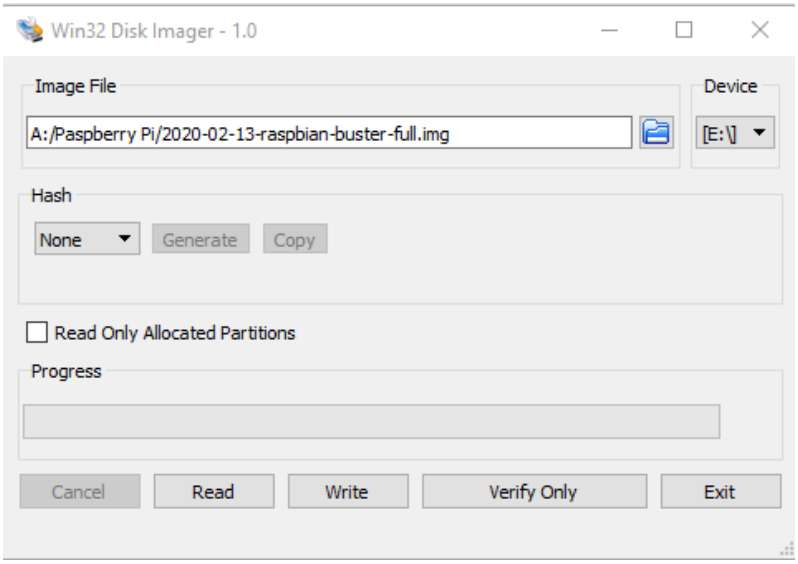

Рис. 2.4 – Встановлення ОС raspbian

2.3 Встановлення, налаштування, оновлення Raspberry Pi

Перед самою установкою слід врахувати, що сама установка займе хвилин 20, а ось перевірка оновлень і їх установка вже може зайняти набагато більше часу від 30 до 50 хвилин реального часу.

І ще один нюанс для raspberry pi потрібен доступ до мережі та промені всього підключити ehternet провід для більш стабільного сигналу інтернету.

Також є варіант віддаленого оновлення пристрою для цього перед вилученням sd картки потрібно в кореневій папці raspberry pi створити файл під назвою SSH і без формату. Тоді після підключення raspberry pi до мережі та зачекавши на установку ми зможемо через putty встановити оновлення та зробити повне налаштування мережевого фільтра.

Але для дипломної роботи я використав більш демонстративний варіант – це запис екрана робочого столу raspberry pi.

2.3.1 Після того як я вставив карту пам'яті SD з iso образом raspbian нас привітає вікно з вибором установки.

Для зручності вибрав установку із графічним інтерфейсом.

2. 3.2 Для зручної роботи із системою вибираю англійську мову. Це дозволить уникнути конфліктів з мовою системи.

2.3.3 У розділі розділення диска вибираю "Guided - use entire disk".

2. 3.4 Далі вибираю розділ SD карти для встановлення на неї системи

2. 3.5 Варто вибрати перший пункт All files in one partition (для більш простої установки)

2. 3.6 Погоджуюся з усіма змінами та продовжую

2. 3.7 Аналогічно попередньому пункту погоджуюсь з усіма змінами у розділі.

2. 3.8 Після всіх угод відбувається встановлення та налаштування системного розділу.

2. 3.9 Узгоджуюсь із встановленням GRUB boot loader для подальшого завантаження системи.

2. 3.10 Тут я вибираю який розділ потрібно відвантажувати

Рис. 2.5 – GRUB boot loader

2. 3.11 Після завершення установки boot loader відбувається перезавантаження.

2. 3.12 Після перезавантаження нас привітає вікно швидкого налаштування системи.

2. 3.13 Вибираю регіонально точні дані, оскільки це допоможе уникнути непотрібних конфліктів.

2. 3.14 Вводимо пароль для облікового запису. Цей пароль буде потрібний для введення команди sudo (від імені адміністратора)

2. 3.15 Автоматичні оновлення я пропустив.

2. 3.16 Це оновлення я проведу стандартним способом. Введіть команду **sudo apt update.**

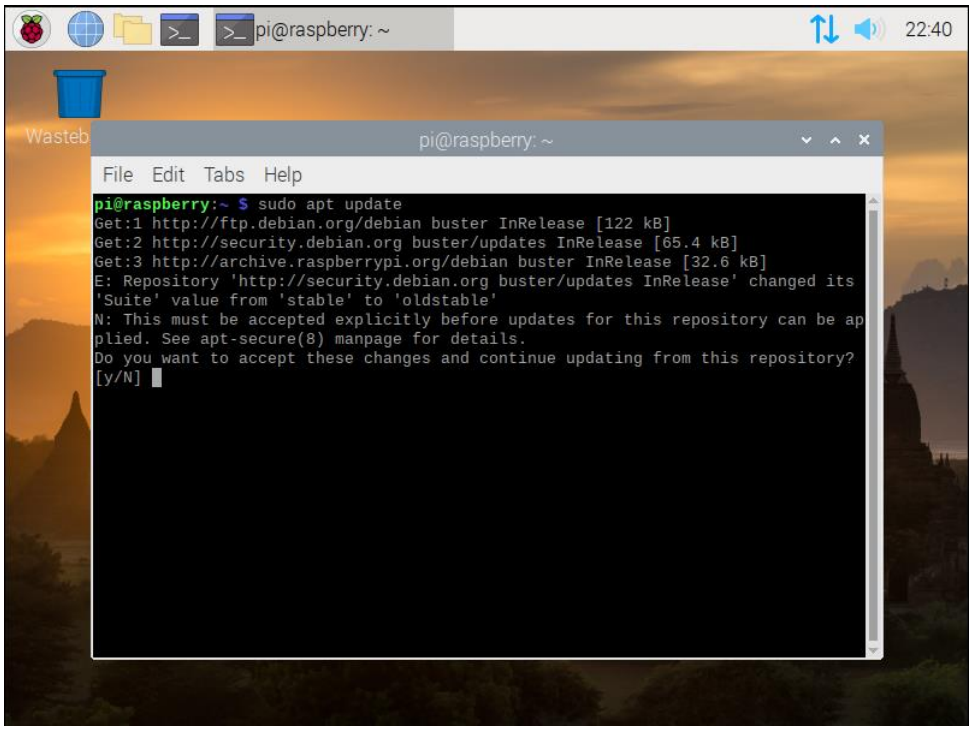

Рис. 2.6 – Оновлення raspberry

2. 3.17 Не виходячи з консолі відразу завершимо оновлення raspberry ввівши ще одну команду **sudo apt upgrade**

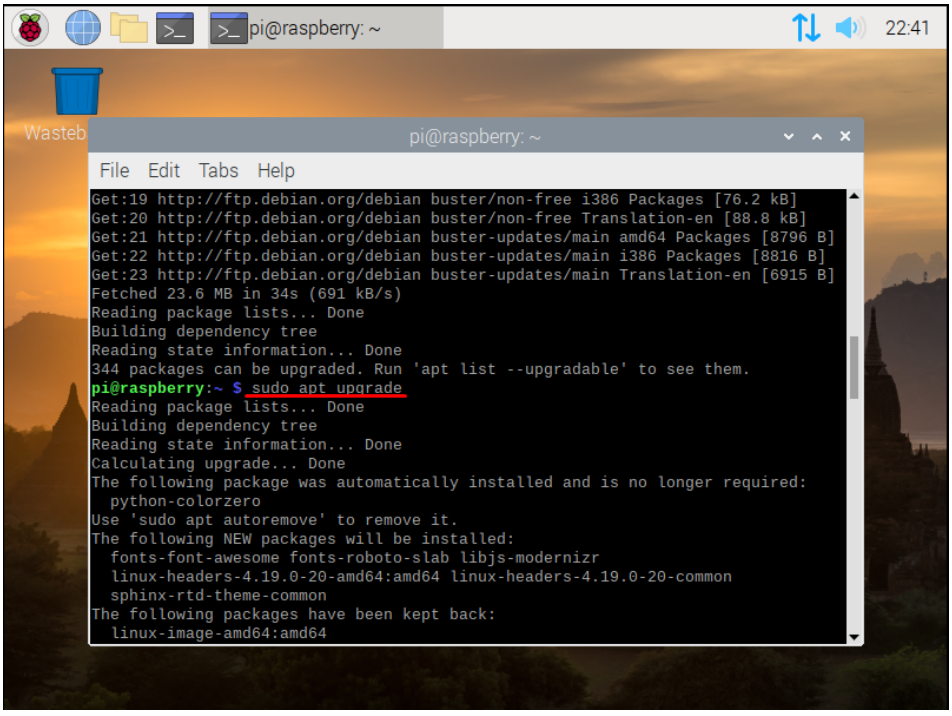

Рис. 2.7 – Завершення оновлення raspberry

2. 3.18 Остання команда займе куди більше часу, але після встановлення вів q у консоль

2.4 Налаштування piHole як первинний мережевий фільтр

Pi-hole — це загальномережевий блокувальник реклами загального призначення, який захищає вашу мережу від реклами та трекерів, не вимагаючи жодних налаштувань на окремих пристроях. Він може блокувати рекламу на будь-якому мережному пристрої (наприклад, смарт-пристроях) і, на відміну від надбудов браузера, Pi-hole блокує рекламу на будь-якому типі програмного забезпечення.

Ось що потрібно знати перед встановленням інструменту pi hole. Так як pi hole це безкоштовна програма з відкритим кодом завантажити його не складе особливих труднощів посилання для скачування я написав у першому пункті цього розділу.

2.4.1 Не перезавантажуючи систему ввів команду (**curl -sSL https://install.pi-hole.net | bash**) для встановлення першого ключового інструменту.

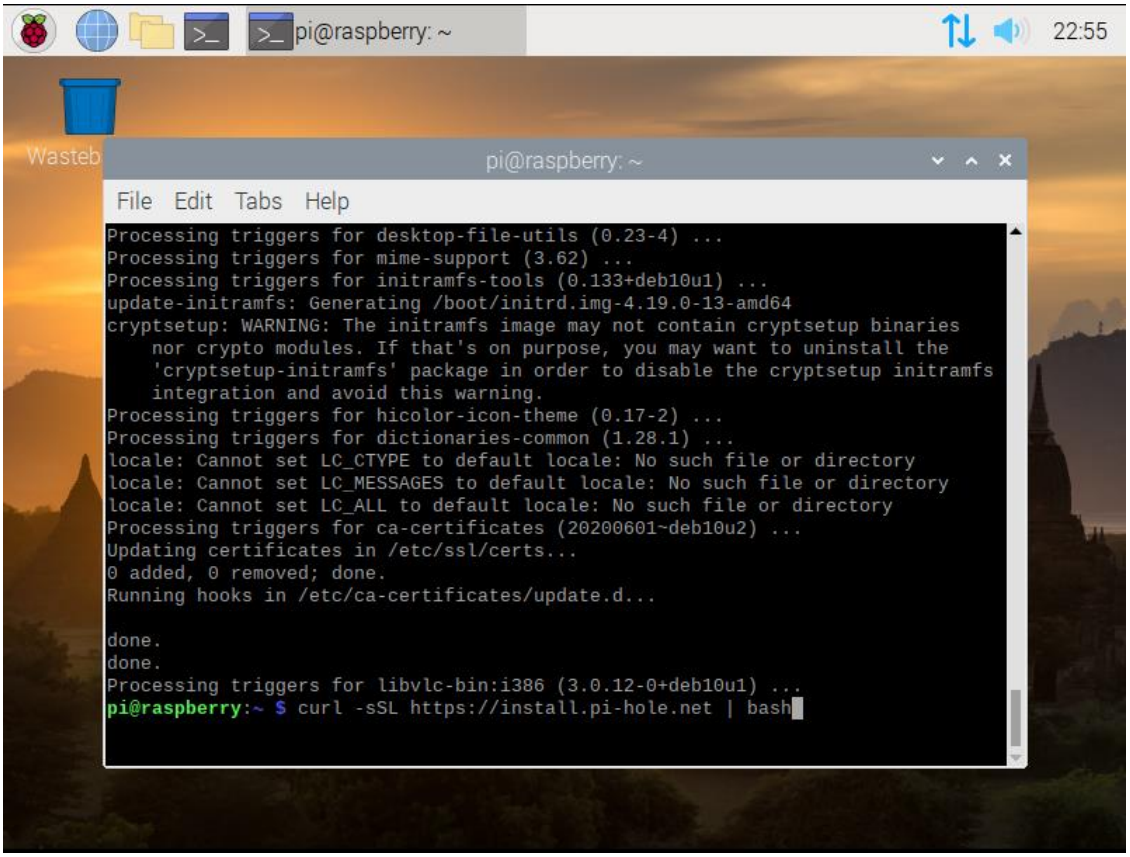

Рис. 2.8 – Установка pi hole

2.4.2 Погоджуюся з тим, що для raspberry pi потрібна статична ip адреса.

2.4.3 Так само погоджуюсь з обраною ip адресою та маскою під мережі

2.4.4 Тут нас попереджають про конфлікт налаштувань роутера та raspberry pi

2.4.5 Кожен із цих пунктів має готовий pool рекламних ресурсів. Для зручності я вибрав Quad9 (filtred, DNSSEC)

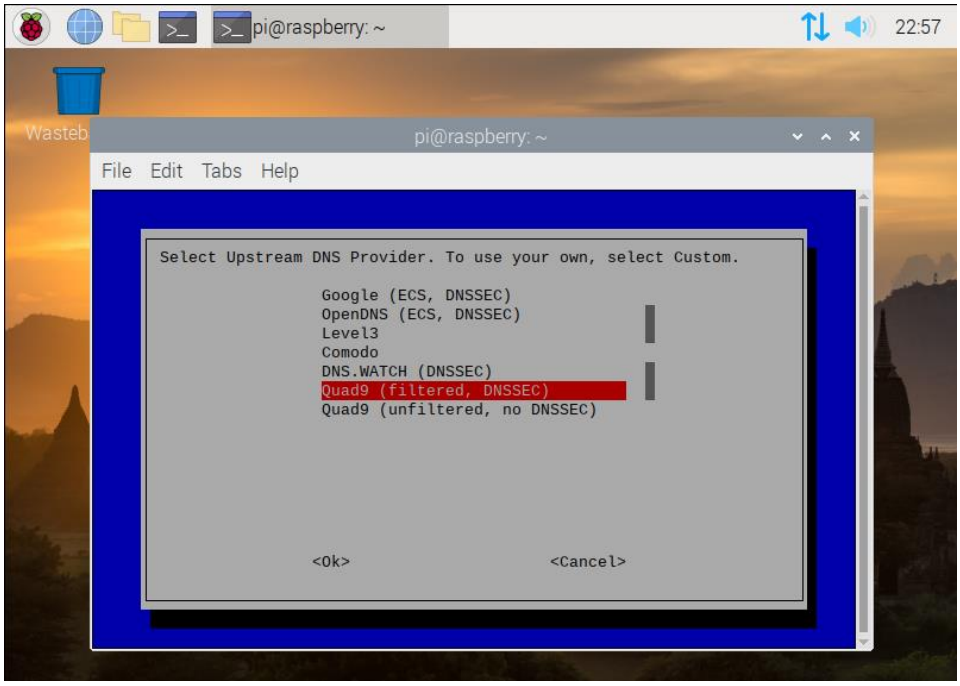

Рис. 2.9 – DNS провайдер

2.4.6 Погоджуюся з обраним листом вже відомих хостів із рекламою.

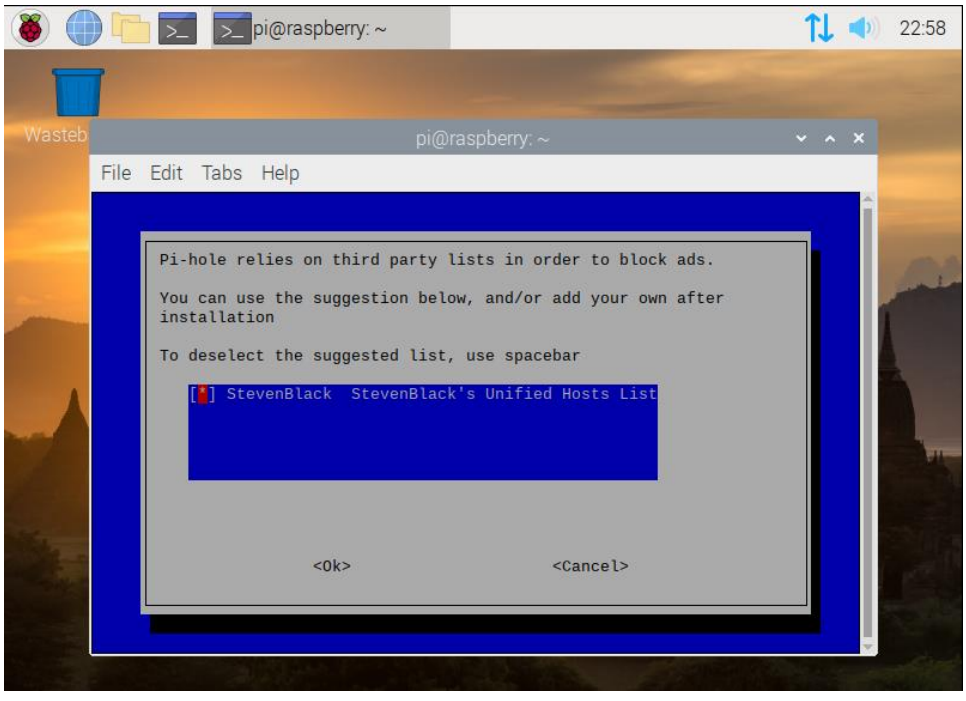

Рис. 2.10 – Hosts list

2.4.7 Для зручності погоджуюсь із встановленням web-інтерфейсу.

2.4.8 Узгоджуюсь із встановленням web сервера **lighttpd**

2.4.9Погоджуюся із записом логів хостів

2.4.10 Вибираю перший пункт для відображення всіх логів

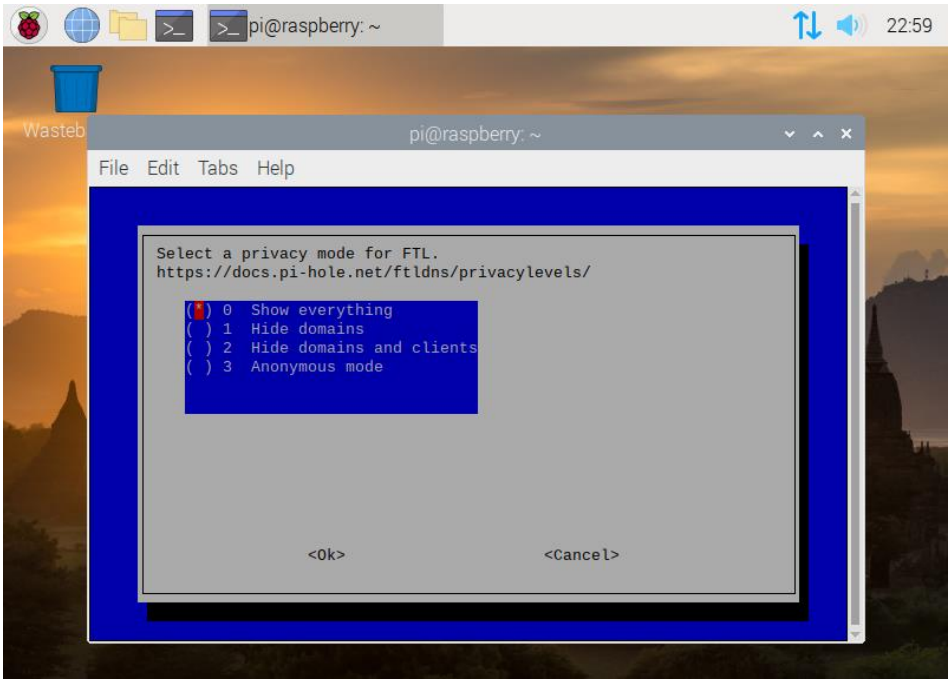

Рис. 2.11 – Рівні приватності

2.4.11 Із закінченням встановлення та налаштування буде згенеровано пароль для входу на сайт

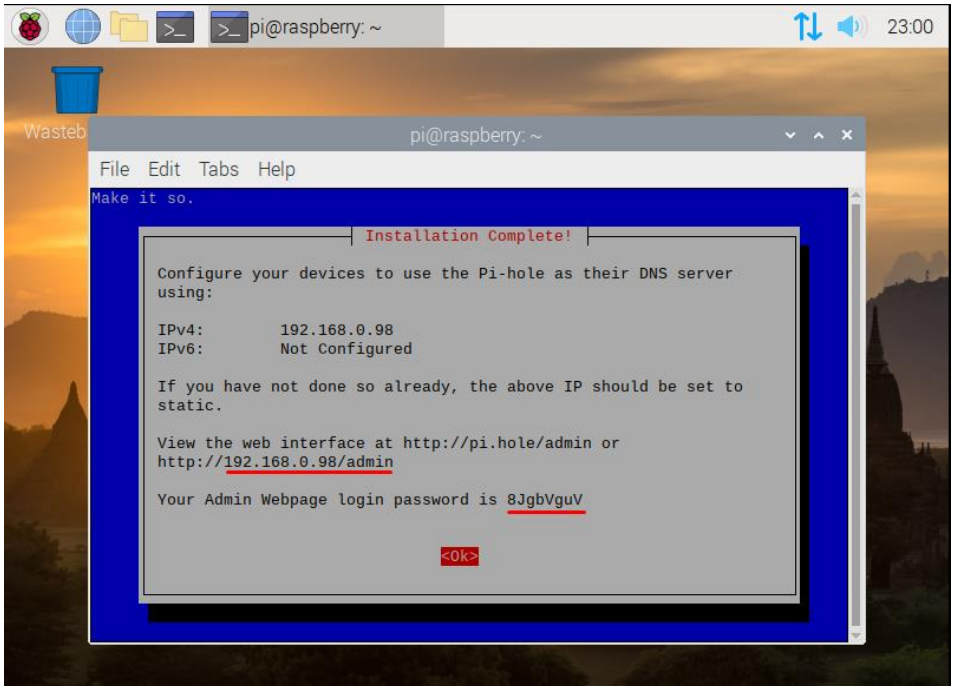

Рис. 2.12 – Логін та пароль

2.4.12 Перейшовши за посиланням або ввівши **192.168.0.98/admin**, авторизуємося на сайті. ip адреса це наша статична ip raspberry pi

2.4.13Після авторизації у нас відкривається повний доступ до перегляду логів сайтів з рекламою доступ до whitelist та групами доступу.

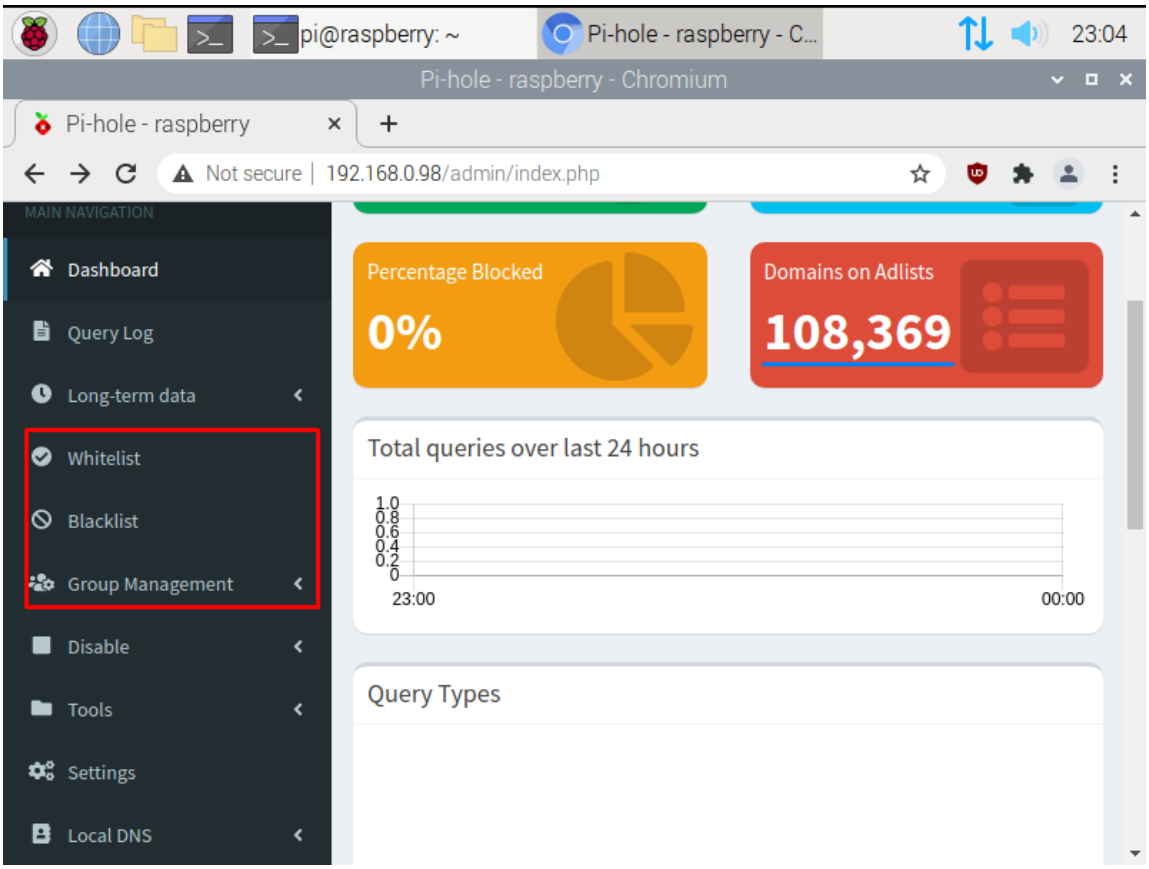

Рис. 2.13– Графічний інтерфейс pi hole

2.5 Створення мережного клієнта та налаштування piVPN

PiVPN — це безкоштовний програмний пакет з відкритим вихідним кодом, який налаштовує сервер VPN з використанням серверного програмного забезпечення OpenVPN. Він був розроблений спеціально для роботи на недорогий Raspberry Pi, хоча повинен працювати на більшості установок Debian.

Pi VPN – це не обов'язкова частина мережевого фільтра. Оскільки вона не виконує суть vpn, анонімність для провайдера. Найкращий спосіб створення vpn це покупка віртуальної машини від Amazon і вже подальше встановлення та налаштування vpn там. Але як і з цим проектом вашої анонімності не буде.

Ваші дані може спокійно переглянути сам Amazon, а у разі цього проекту провайдер може видати вашу історію уряду.

2.5.1 Після встановлення pi-hole почну установку vpn, ввівши посилання (**curl -L https://install.pivpn.io | bash**)

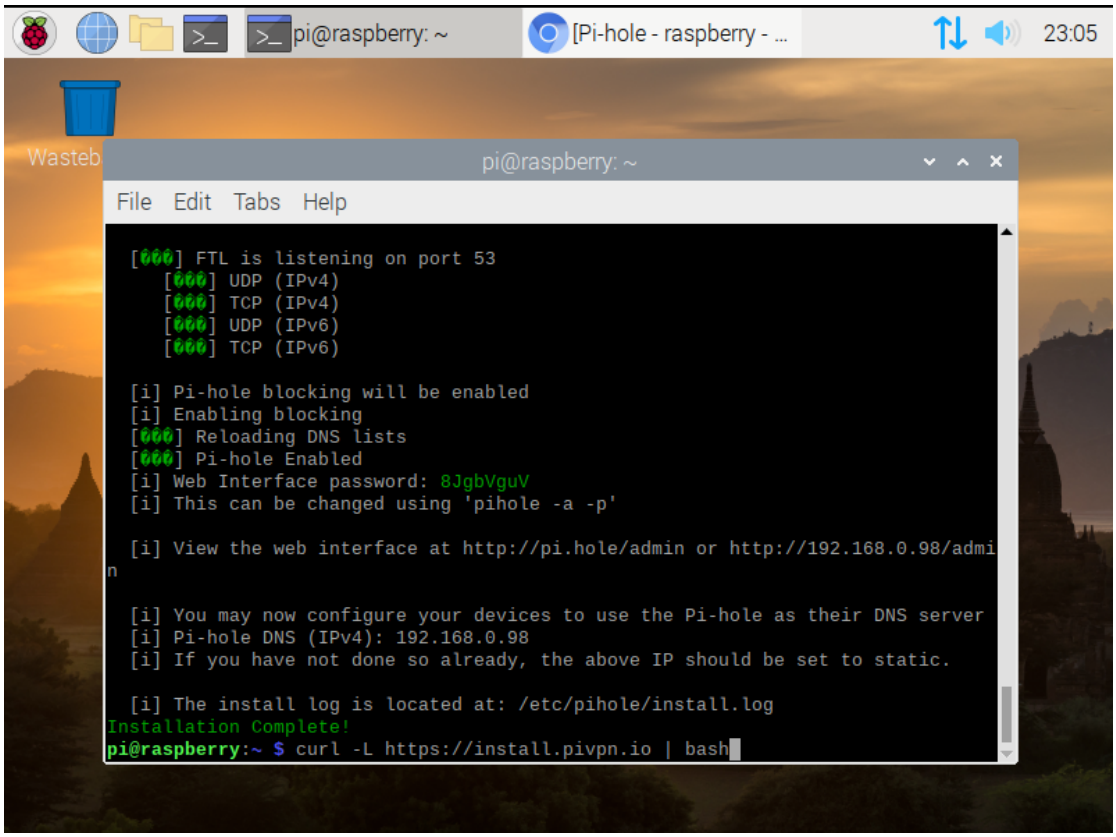

Рис. 2.14 – Встановлення pi vpn

2. 5.2 Нас привітає віконце з попередженням про трансформацію пристрою на сервер vpn. Це не завадить роботі нашого сервера adblock.

2. 5.3 Тут також говориться про необхідність статичної ip адреси

2. 5.4 Вибираю користувача, який буде зберігати vpn налаштування

2.5.5 Вибрав стандартного користувача

2.5.6 Для зручної роботи я не змінюватиму мережеві протоколи і залишу за стандартом **UDP** протокол

2.5.7 За стандартом відкритий VPN **UDP протокол це 1194**. У першому розділі йшлося про те, що його промені не використовувати. Але оскільки це дипломний проект, я залишу його за замовчуванням

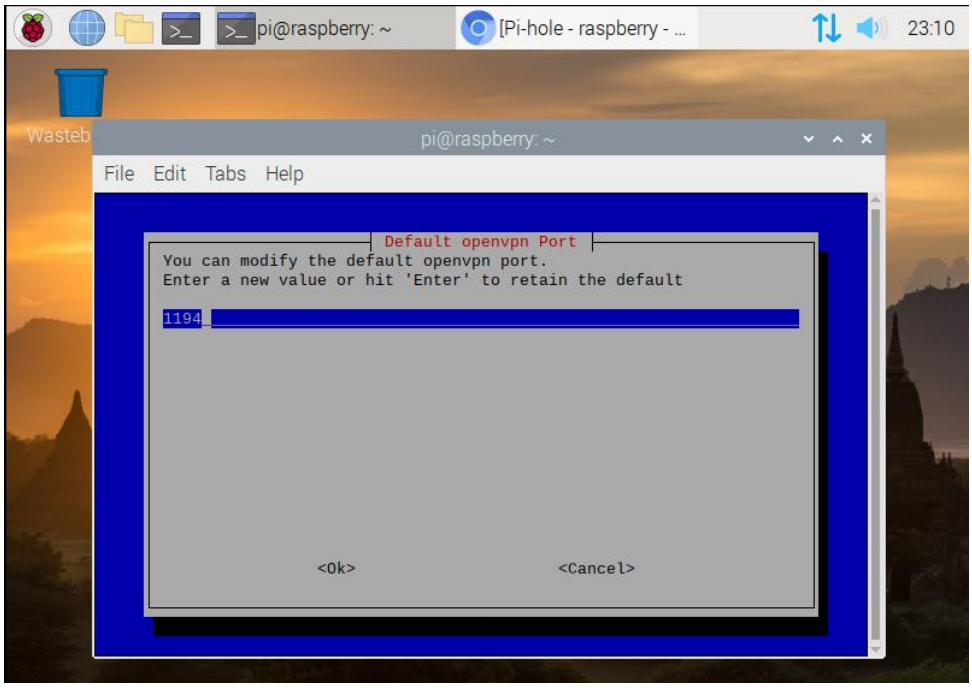

Рис. 2.15 – Введення відкритого порту

2.5.8 Тут мене ще раз попереджають про коректність запровадженого протоколу

2.5.9 Розумію що я вже маю один **DNS server** це перший сервер з AD-Block . Так як я використовую UDP протокол на ту ж ip адресу конфліктів не буде

2.5.10 Для чистоти роботи, як було написано в першому розділі, варто використовувати **білу ip** адресу.

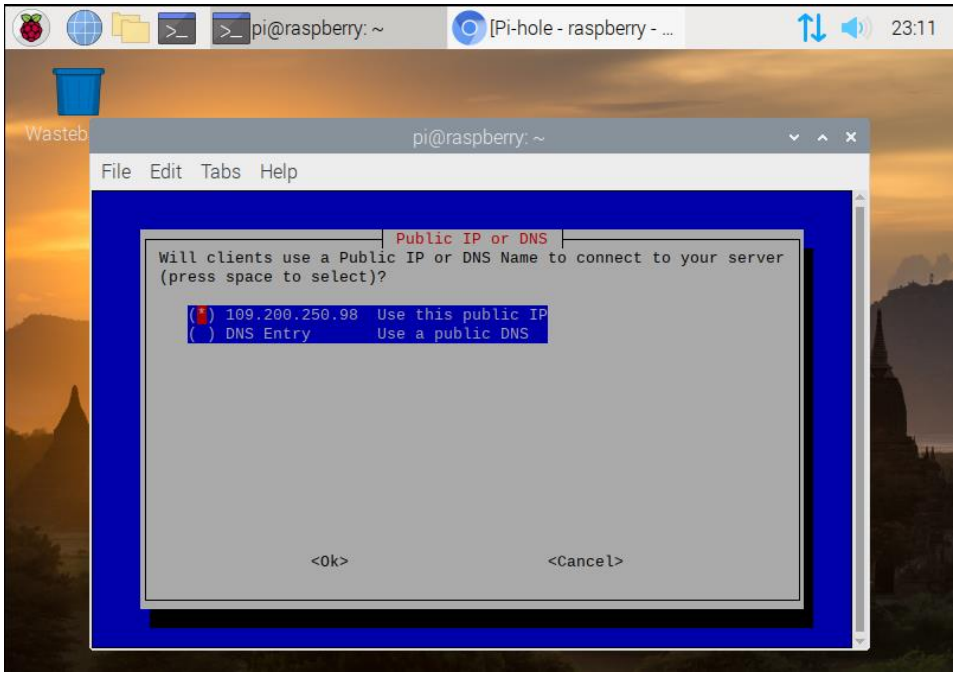

Рис. 2.16 – Вибір білої ip адреси

2.5.11 Починається генерація HMAC ключа, за яким можна буде легко підключитися.

2.5.12 Це попередження про оновлення і те, що система не перезапускатиметься

2.5.13 Погоджуюся з автоматичним встановленням оновлень

2.5.14 Завершуємо встановлення pi-VPN

2.5.15 Та перезапускаю raspberry pi

2.6 Підготовка VPN ключа

VPN ключ — це рядок символів, який використовується як ключ автентифікації. Можемо використовувати попередньо спільні ключі для перевірки автентичності між сайтами VPN та сторонніми VPN-клієнтами.

Обидва шлюзи створюють хеш-значення на основі загального ключа та іншої інформації. Потім хеш-значення обмінюються та перевіряються для аутентифікації іншої сторони.

Як випливає з назви, загальний ключ має бути заздалегідь поширений на всі пристрої, які його використовують. VPN ключі повинні передаватися конфіденційно, тому що їх переваги безпеки негайно губляться, якщо ключ розкривається неавторизованим сторонам.

У цьому проекті vpn ключ буде не лише зашифровано, але ще й захищено унікальним паролем для його активації. Так що якщо наші користувачі "втратять" або віддадуть ключ, то у зловмисника буде лише файл із набором символом.

2.6.1 Після перезапуску запускаємо консоль та вводимо команду **pivpn add**. Вводимо ім'я клієнта, скільки він буде працювати та надійний пароль для доступу, якщо ключ потрапить в чужі руки.

2.6.2 Після завершення створення клієнта в **/home/pi/ovpns** згенерується ключ для OpenVPN, цей файл можна перекидати на будь-який пристрій і підключаться.

2.6.3 Сам файл матиме наступний формат

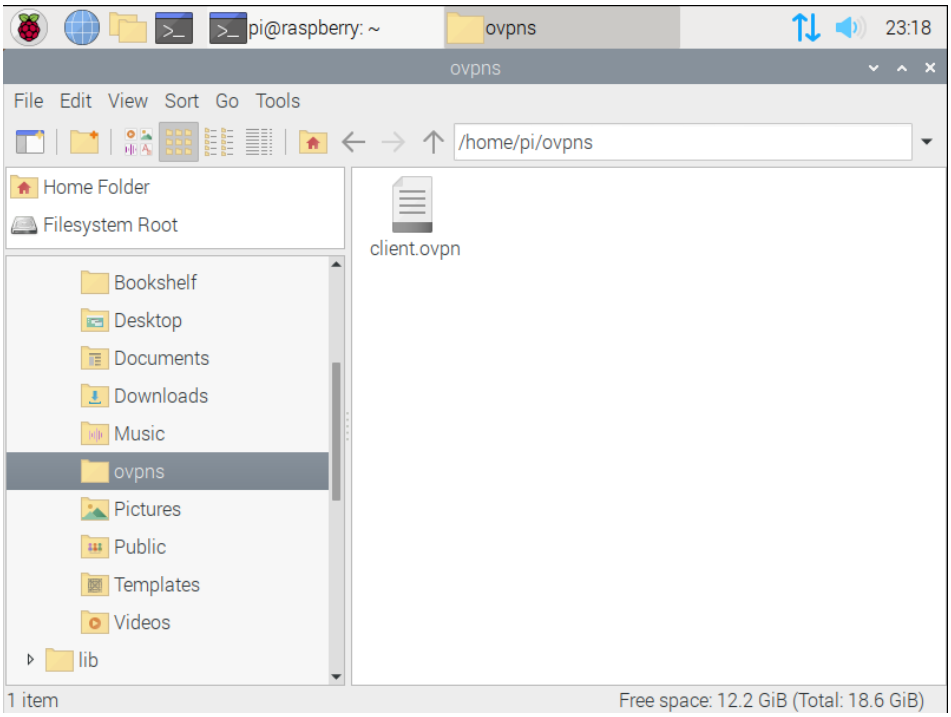

Рис. 2.17 – Каталог з client.ovpn

2.6.4 Вже на тестовій віртуальній машині завантажуємо наш файл та OpenVPN

2.6.5Але спочатку перевіримо працездатність блокувальника реклам. Перейдемо в **центр управління мережами та спільним доступом**

2.6.6 У вікні, що відкрилося, вибираю "**Зміна параметрів адаптера**" і натиснувши ПКМ по **мережному адаптеру** вибираю властивості

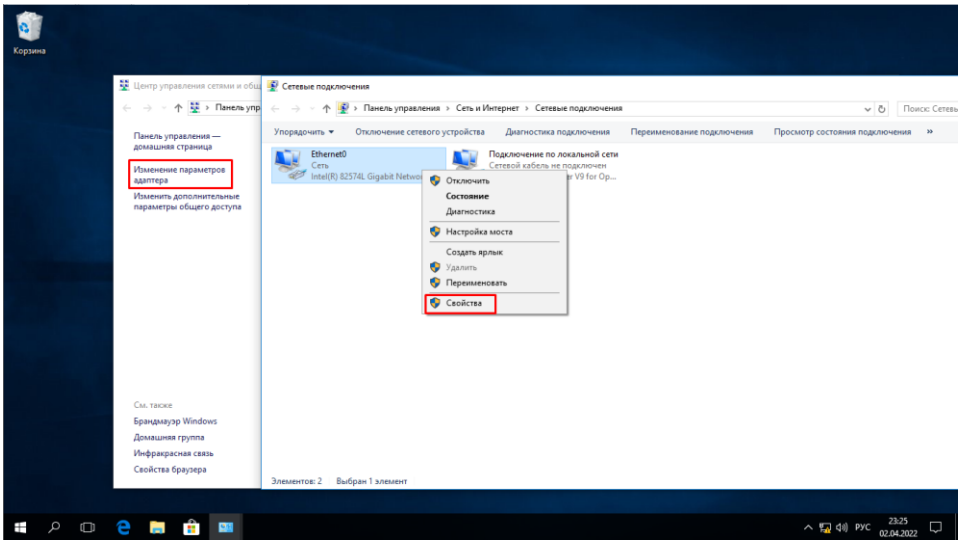

Рис. 2.18 – Зміна параметрів адаптера

2.6.7 Переходжу в IPv4 і як DNS вводжу статичний ip адресу raspberry pi

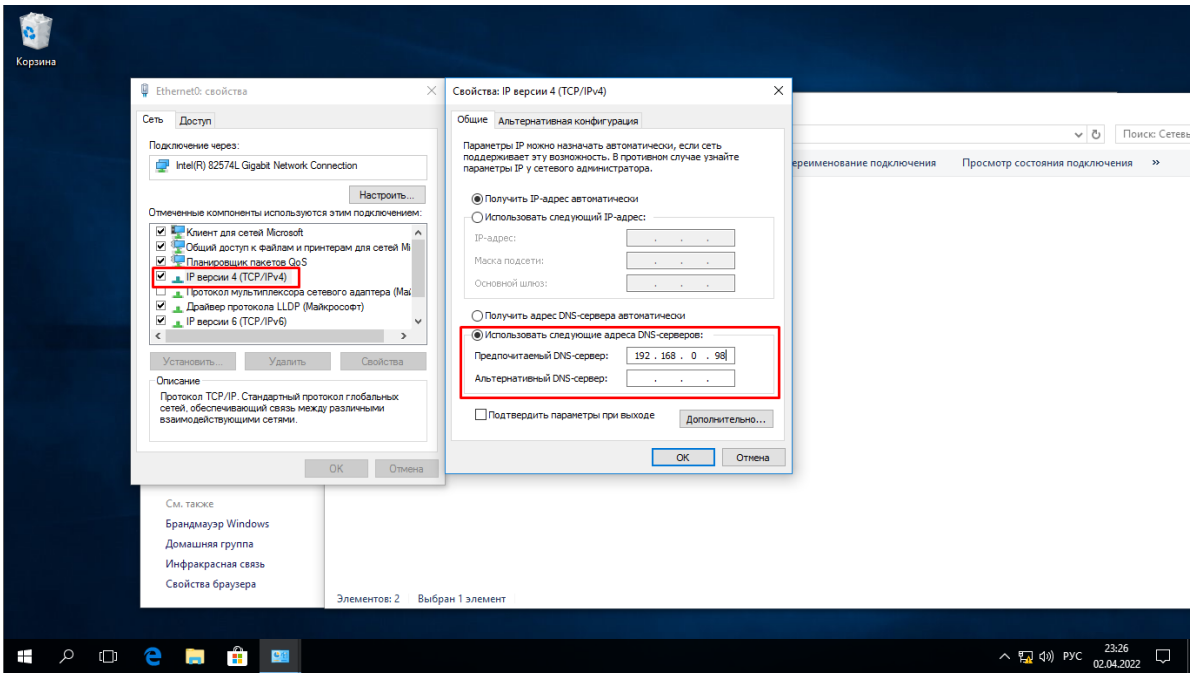

Рис. 2.19 - Зміна параметрів на статичний ip

2.6.8 Крім виділення статичної адреси роутером можна так само ввести його через графічний інтерфейс raspberry і так само ввести як DNS сервер ip адресу цієї raspberry pi

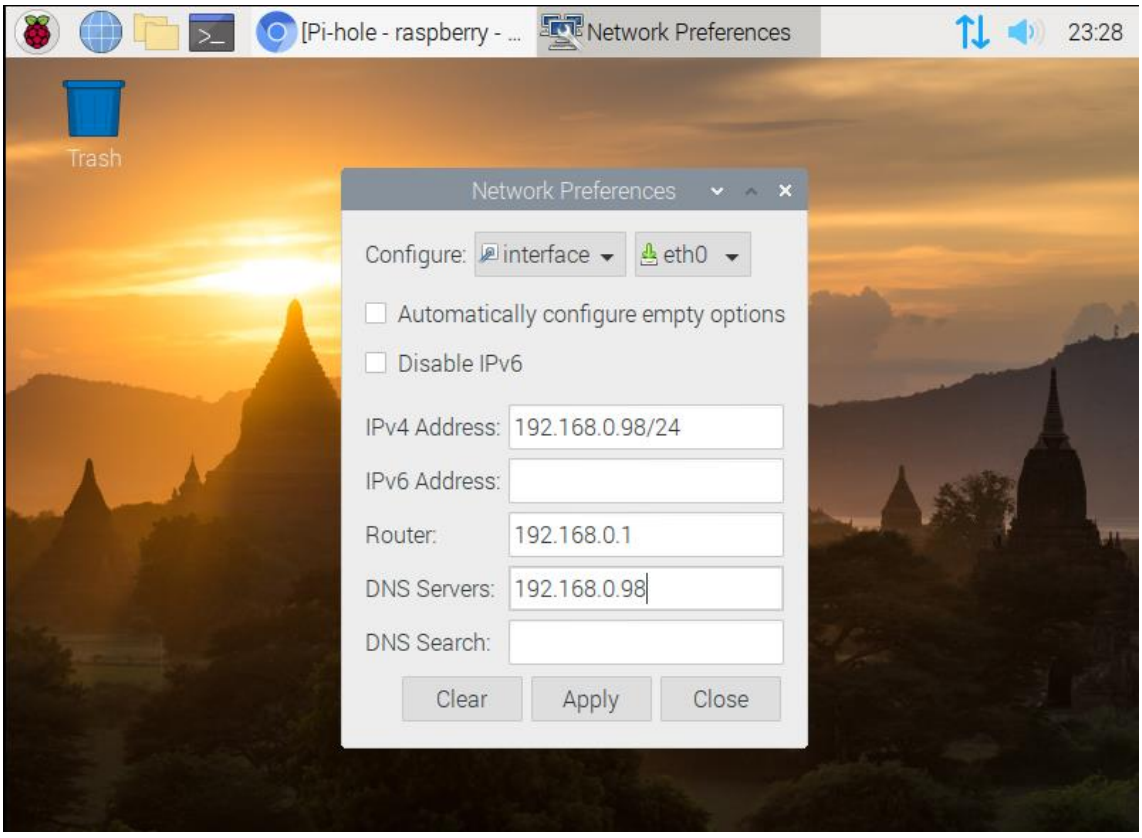

Рис. 2.20 – Настройка ip на raspberry pi

2.6.9 Тут на прикладі сайту OpenVPN можна побачити, що доступ до мережі присутній і реклама відсутня

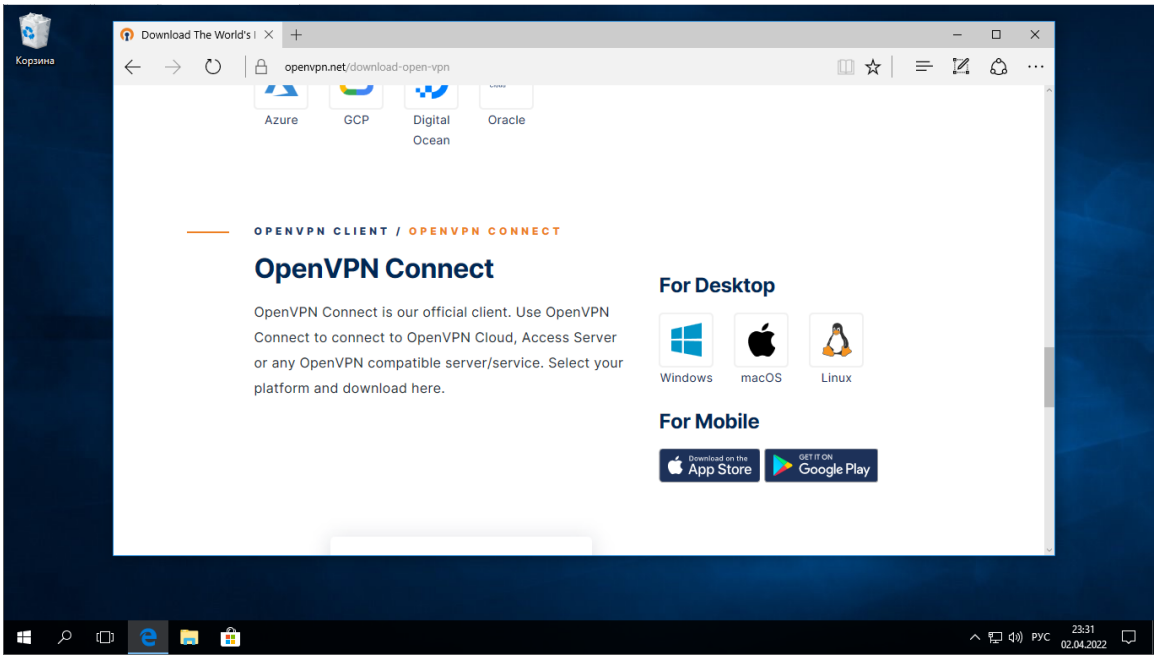

Рис. 2.21 – Працездатність блокувальника

2.6.10 Для підключення пристрою до VPN запускаю програму OpenVPN і перетягую завантажений файл із raspberry pi.

2.6.11 І після того, як я ввів зручне для мене ім'я профілю та пароль від ключа клієнта, можна спокійно підключитися.

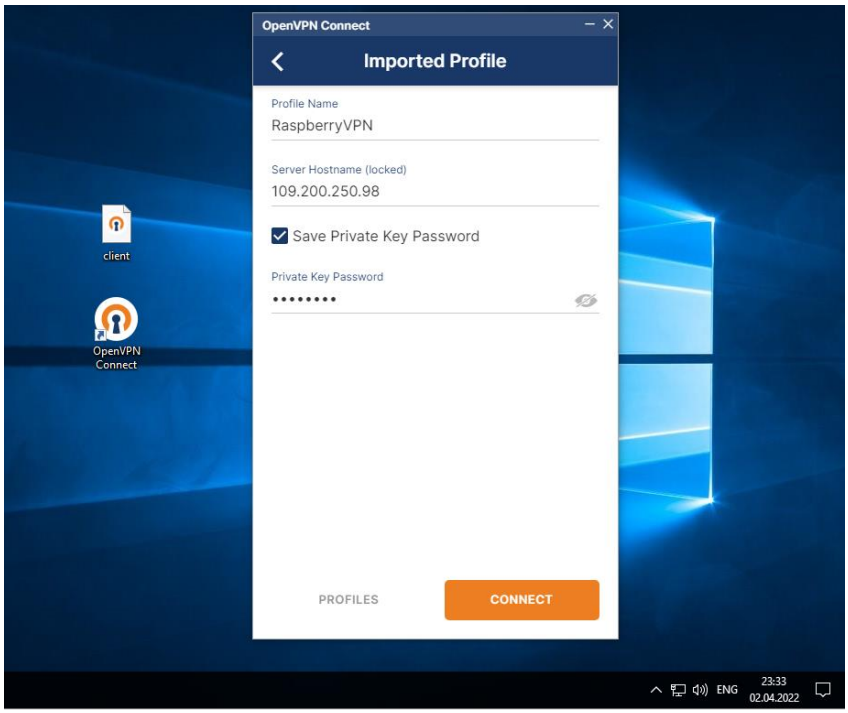

Рис. 2.22 - Графічний інтерфейс vpn

2.7 Налаштування мережного маршрутизатора

В рамках даної роботи я вибрав маршрутизатор tp-link, оскільки він є більш поширеним, ніж інші роутери. Варто врахувати, що налаштування роутера є фундаментом для нашої мережі. Оскільки якщо не відкрити порти, то доступ до нашого мережевого фільтра буде лише у локальної мережі і без адекватного vpn.

2.7.1 Натиснувши ctrl + r і ввівши cmd відкриється терменал туди потрібно ввести команду ipconfig. Після цього нам видасть інформацію про наш шлюз, який потрібно ввести в браузер, щоб перейти до налаштувань роутера.

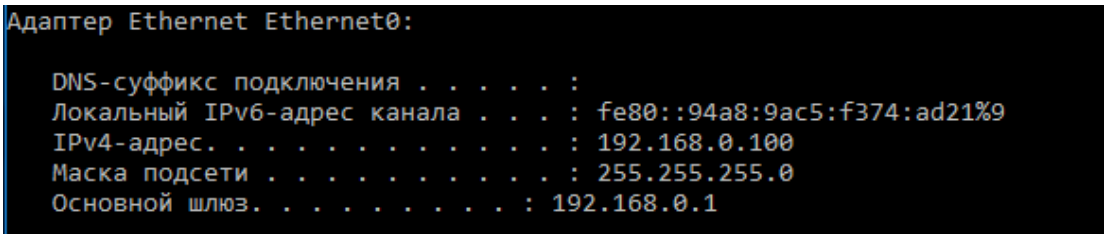

Рис. 2.23 – Налаштування адаптера

2.7.2 Резервуємо ip адресу на роутері. Для цього перейшовши в мережевий інтерфейс пристрою переходжу на вкладку DHCP, а там Резервування адрес

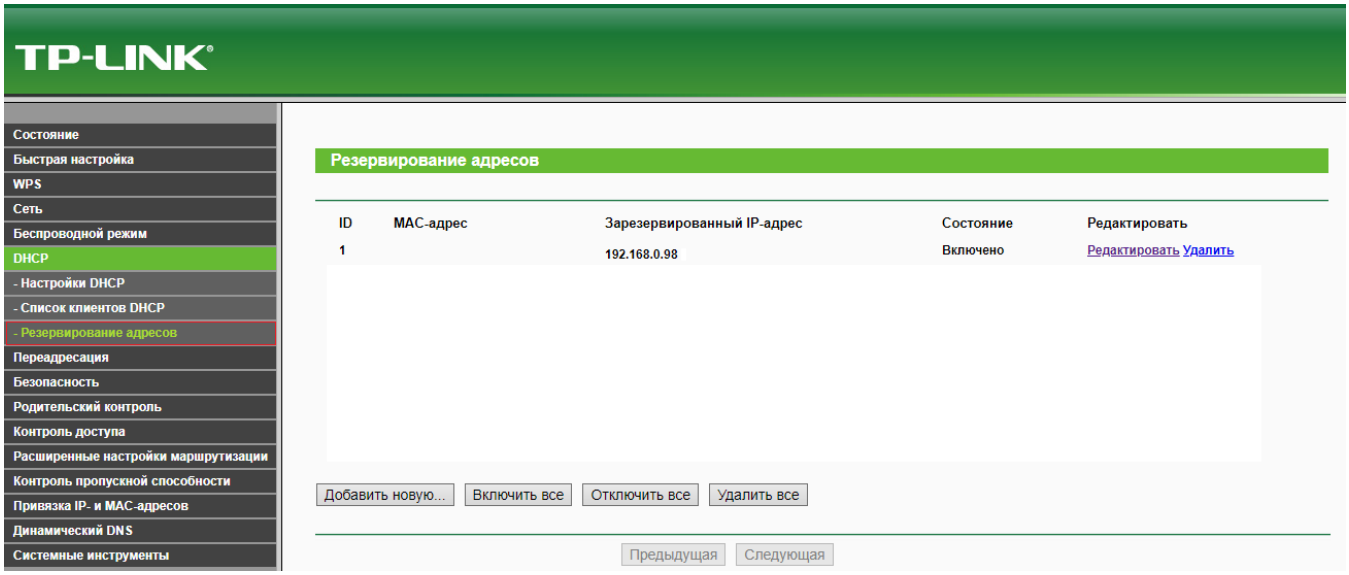

Рис. 2.24 - Налаштування DHCP

2.7.3 Вводжу ip адресу та MAC адресу пристрою

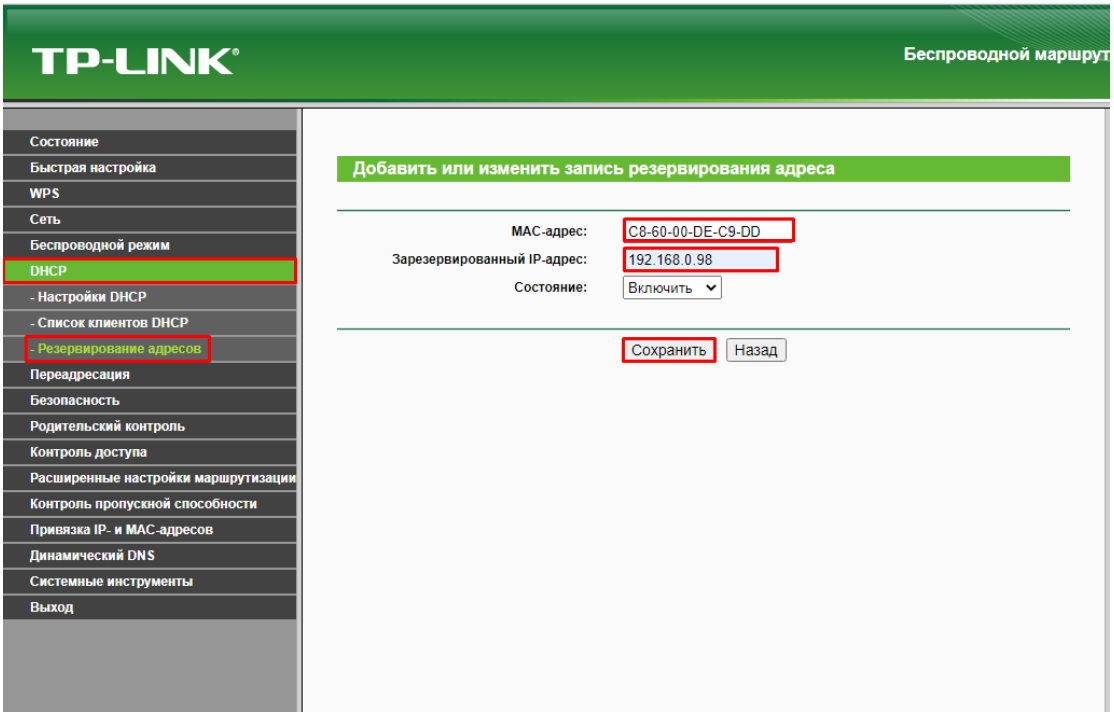

Рис. 2.25 - Резервація MAC адреси

2.7.4 Відкриваю порт для доступу до vpn. Переходимо в Переадресація , Віртуальні сервери та натискаю Додати

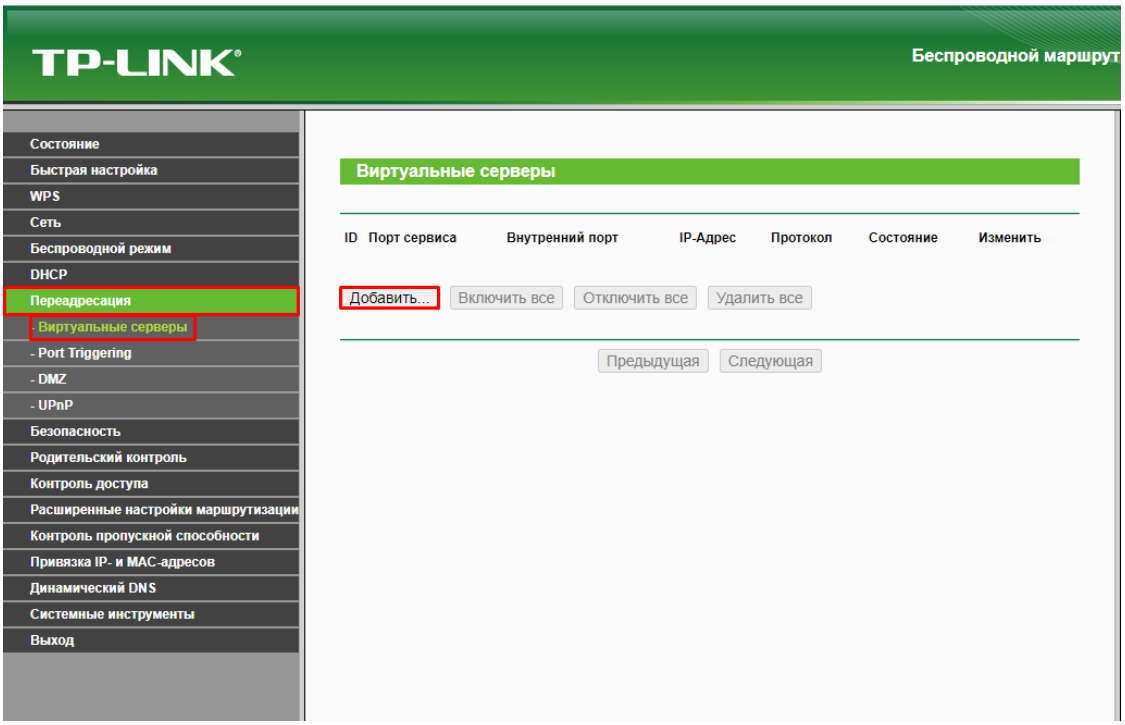

Рис. 2.26 - Відкриття мережевого порту

2.7.5 Далі вводжу виділений порт і наш IP адрес залишаю повний доступ по всіх протоколах і включаю його.

РОЗДІЛ 3. ТЕСТУВАННЯ РОБОТИ МЕРЕЖЕВОГО ФІЛЬТРУ

3.1 Тип загроз для мережевого фільтра

Мережеві загрози бувають двох типів:

Пасивні мережні загрози: такі дії, як прослуховування телефонних розмов та сканування в режимі очікування, призначені для перехоплення трафіку через мережу.

Активні мережеві загрози: такі як, атака (DoS) та атаки з впровадженням SQL, коли зловмисник намагається виконати команди, щоб порушити нормальну роботу мережі.

Два найбільш поширені варіанти використання пасивних атак:

1. Аналіз трафіку. У цьому типі зловмисник відстежує канали зв'язку для збору різної інформації, включаючи особисті дані людини та машини, місцезнаходження цих посвідчень та типи використовуваного шифрування, якщо це застосовується.

2. Розголошення вмісту повідомлення. У цьому випадку зловмисник відстежуватиме незахищене середовище передачі даних, наприклад незашифровану електронну пошту або телефонний дзвінок, та перехоплюватиме її для отримання конфіденційної інформації.

Виявити пасивну атаку дуже складно, а у багатьох випадках неможливо, тому що вона жодним чином не пов'язана зі зміною даних. Тим не менш, ви можете вжити захисних заходів, щоб зупинити його, в тому числі:

Використання методів шифрування для шифрування повідомлень, що робить їх нечитаним для непередбачуваних одержувачів. В цьому випадку

можуть бути реалізовані два типи шифрування:

1.Симетричні ключі (один і той самий ключ на обох кінцях) — ми ще маємо проблему таємного обміну секретним ключем.

2.Шифрування з відкритим ключем, при якому кожна сторона (чи то користувач, програма або система), що бере участь в обміні даними, має два ключі, один відкритий і один приватний, які повинні зберігатися в секреті. Прикладом цього є використання SSL/TLS-сертифікати (HTTPS), які використовуються для забезпечення достовірності ідентифікації комп'ютерів між веб-сервером і чиїмось браузером.

Уникайте публічного розміщення конфіденційної інформації (наприклад, приватної інформації та інформації про компанію), яка може бути використана сторонніми хакерами для проникнення у вашу приватну мережу.

На відміну від пасивної атаки, активну атаку з більшою ймовірністю буде швидко виявлено метою після її виконання. Нижче наведено деякі заходи захисту від цього типу атак:

1.Може бути згенерований випадковий сеансовий ключ, який дійсний тільки для однієї транзакції за раз, це має ефективно запобігти повторній передачі вихідного повідомлення зловмисником після завершення вихідного сеансу.

2.Використання одноразових паролів допомагає автентифікувати транзакції та сеанси між сторонами, що взаємодіють. Це гарантує, що навіть якщо зловмиснику вдалося знову записати і повторно передати захоплене повідомлення, термін дії пов'язаного з ним пароля закінчиться.

3.Використання протоколу автентифікації Kerberos (зазвичай використовується в Microsoft Windows Active Directory), який підтримує безліч заходів протидії різним типам атак відтворення.

3.2 Моделювання загроз мережевої безпеки

Реалізація **<u>виправленої</u>** вразливості

Відбитий міжсайтовий скриптинг – неправильна нейтралізація введення під час створення веб-сторінки

В результаті віддалений користувач може впровадити довільний веб-скрипт або HTML-код через неправильне очищення даних, наданих користувачем, та здійснити атаку відображеного міжсайтового скриптингу проти інших користувачів та вкрасти файл cookie сеансу.

Покрокова інструкція

Зловмисник може створити HTTP-запит і відправити його користувачеві, що пройшов автентифікацію в Pi-hole, щоб впровадити довільний веб-скрипт або HTML в заголовок HTTP Origin, що відображає введення користувача.

Користувачеві пропонується клацнути шкідливу сторінку з кодом JavaScript, щоб виконати наступний HTTP-запит у браузері жертви:

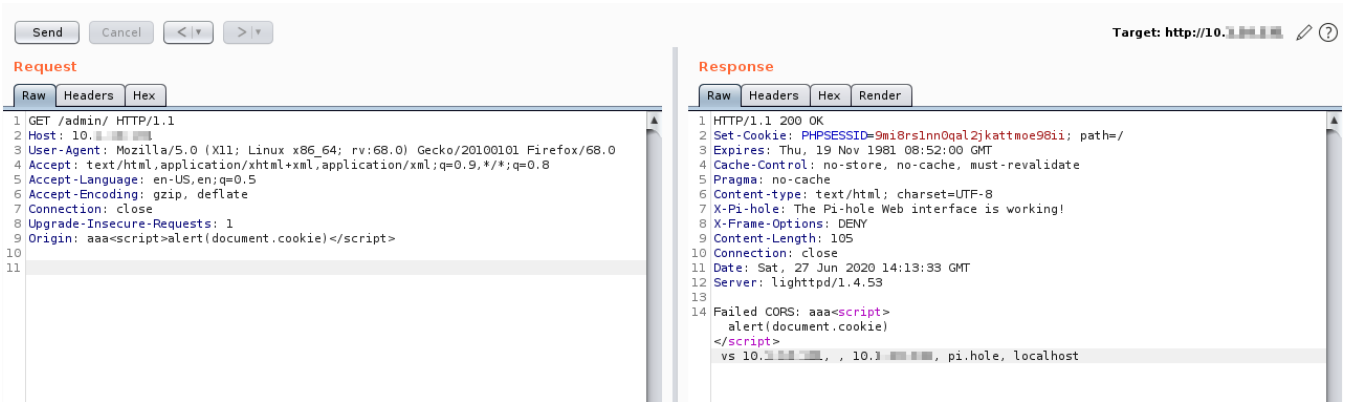

Рис. 3.1 – Target

Корисне навантаження XSS відображається на екрані.

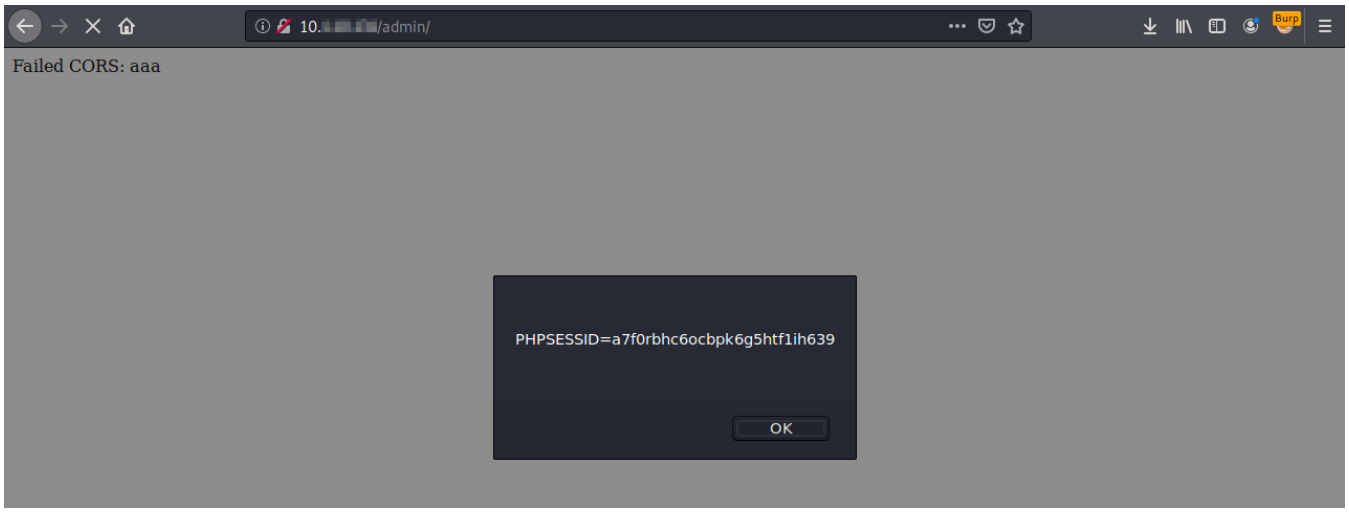

Рис. 3.2 – Корисне навантаження

Важливо, що файл cookie сеансу PHPSESSID не має прапора HttpOnly при першому призначенні користувача:

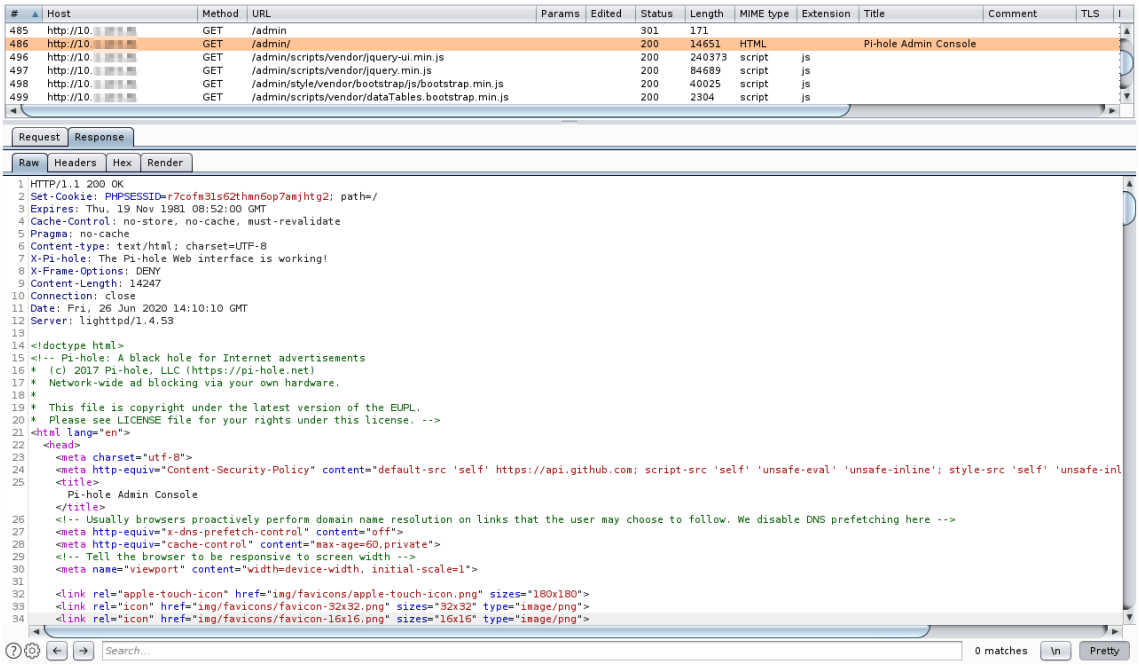

Рис. 3.3 – PHPSESSID

Вплив на безпеку

Використовуючи цю проблему, зловмисник може націлити користувача на кілька типів прямих або непрямих впливів, таких як крадіжка облікових даних, порушення цілісності та різні типи фішингових атак. Цей тип відображеного XSS потребує взаємодії з користувачем.

3.3 Результати тестування мережевого фільтру

Підключивши тестову машину до мережного фільтра можна побачити що без особливого навантаження на загальну мережу , стабільність цієї мережі та її швидкість ні як не впала нижче представлений скріншот з перевіркою швидкості мережі

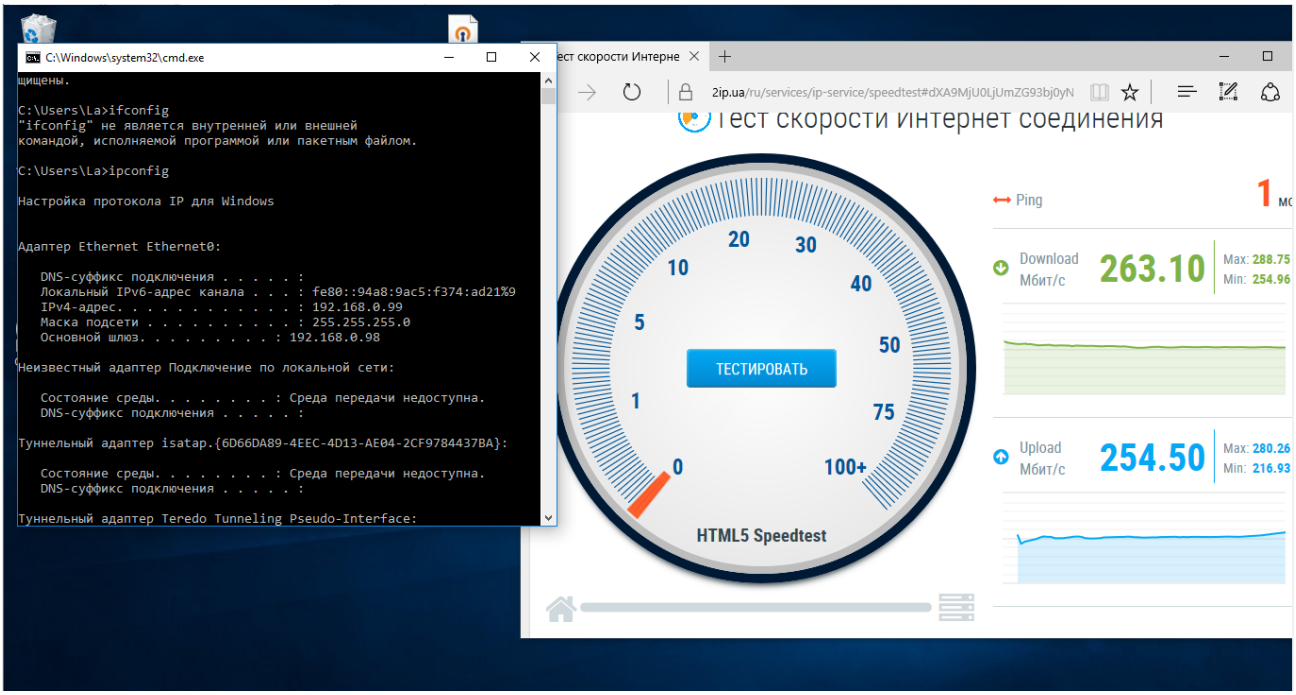

Рис. 3.4 – Перевірка швидкості мережі

Нижче наведено скріншот піратського сайту з нинішнім трендом. Як видно на скріншоті відсутня реклама

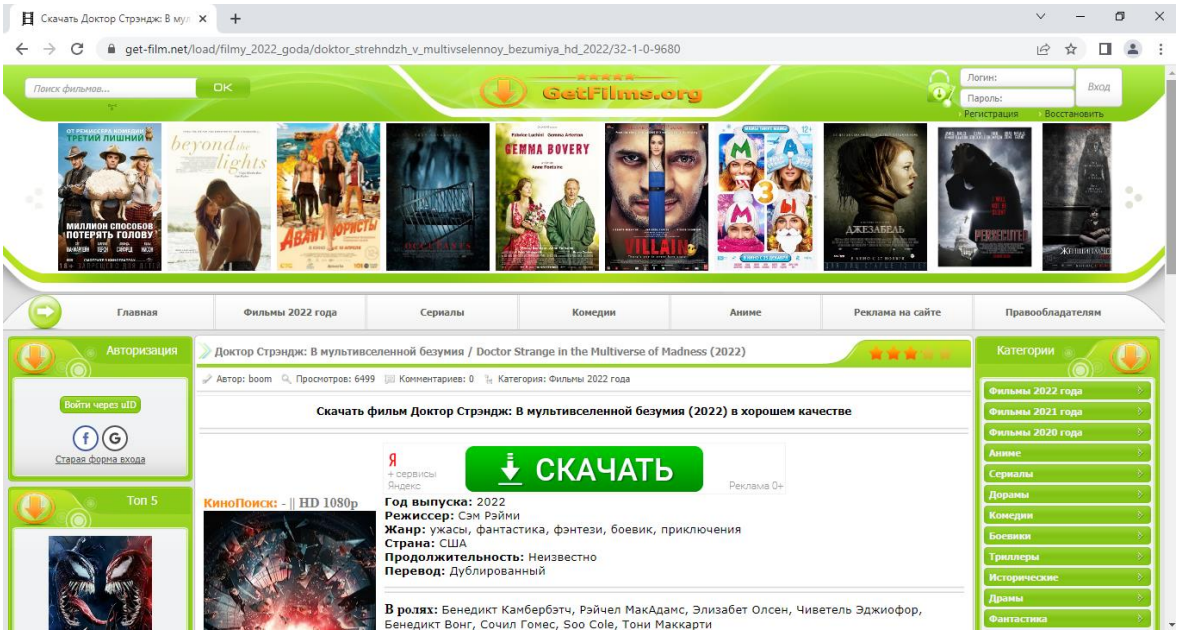

Рис. 3.5 – Піратський сайт без реклами

Робота з blacklist та Query Log

Переходимо в blacklist і як приклад додаємо домен google

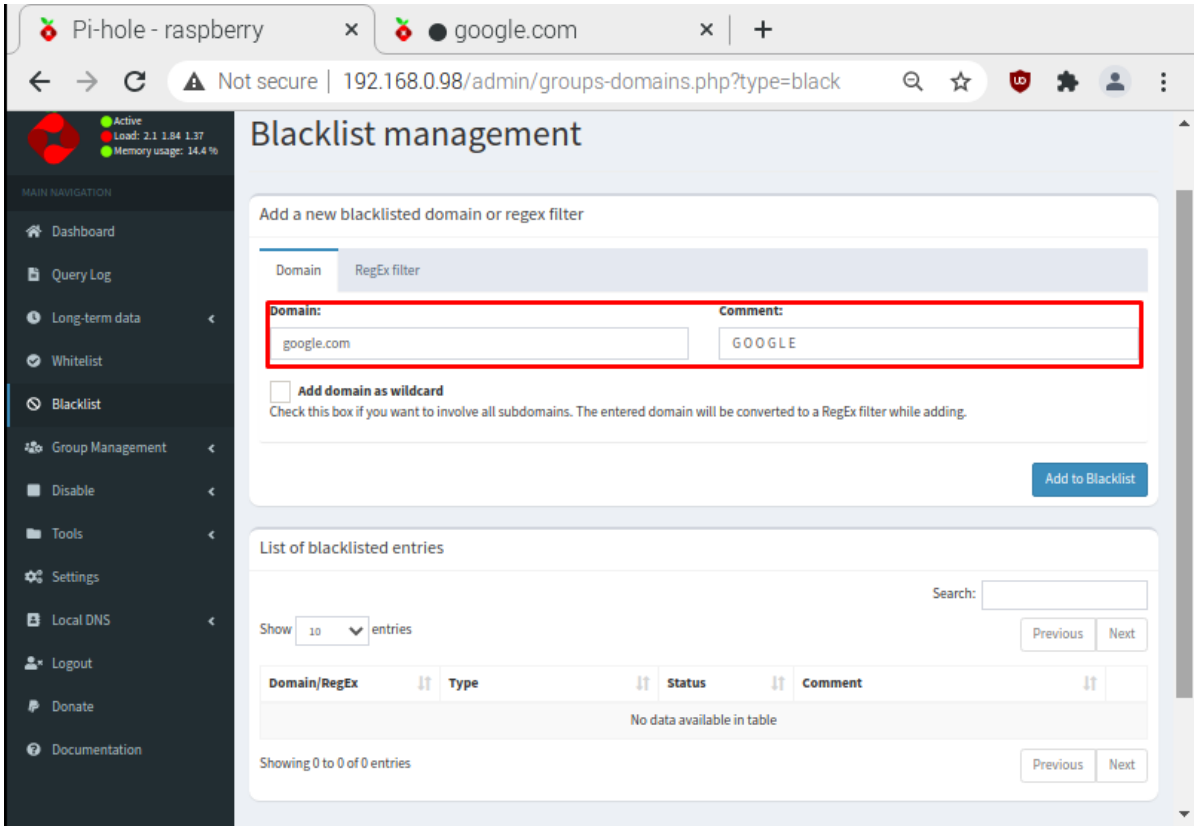

Рис. 3.6 – Blacklist

Після натискання Add to Blacklist ми можемо побачити результат на наступному сриншоті

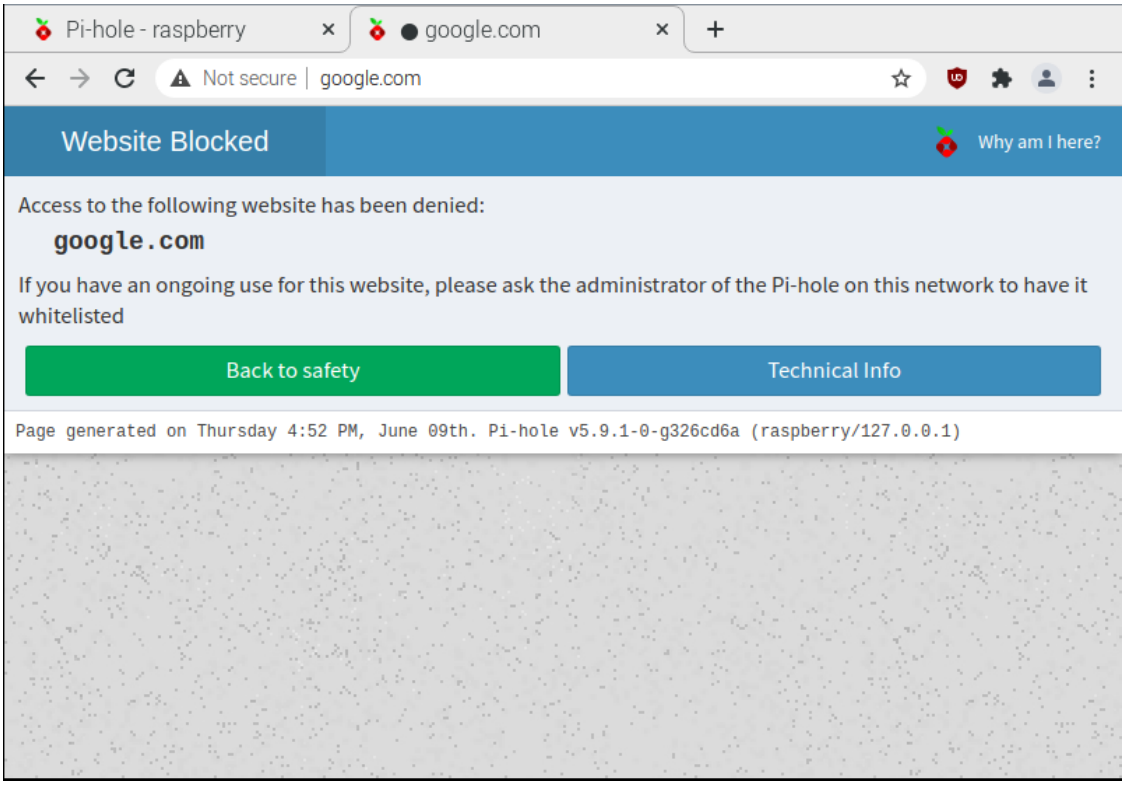

Рис. 3.7 – Заблокований сайт

Робота з whitelist аналогічна blacklist тільки надає доступ до сайтів

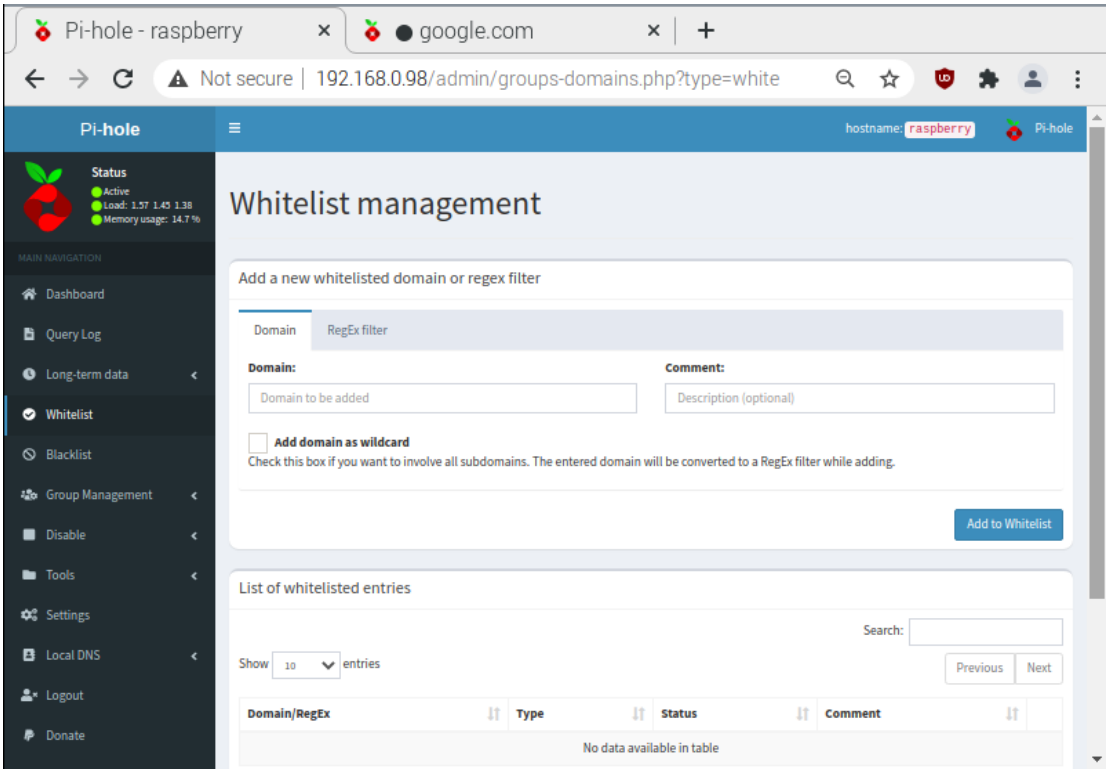

Рис. 3.8 – Whitelist

Також є більш зручний спосіб обмежувати доступ до доменів використовуючи **Query Log**

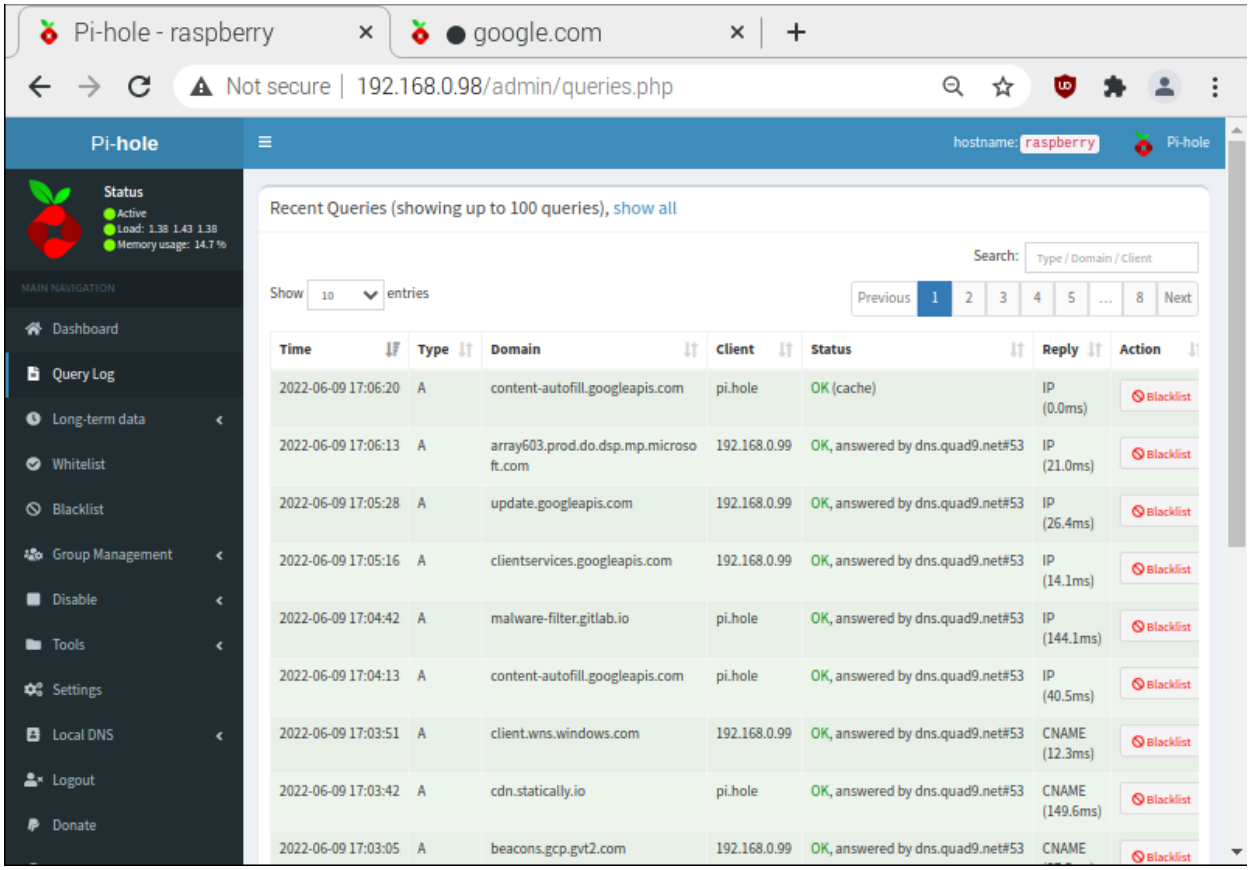

Рис. 3.9 – Logs

РОЗДІЛ 4. ОХОРОНА ПРАЦІ

ВСТУП

Загальними законами України, що визначають основні положення з охорони праці є Конституція України, Закон України «Про охорону праці», Кодекс Законів про Працю України, Закон України «Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності» тощо.

Відповідальність за забезпечення безпечних умов праці, дотримання законодавства по охороні праці покладається на керівника підприємства (роботодавця). На робітників та службовців покладаються обов'язки по дотриманню всіх інструкцій з охорони праці, правил по обслуговуванню машин, правильному застосуванню засобів індивідуального захисту.

4.1Аналіз небезпечних та шкідливих чинників, що впливають на працівника.

Дипломним проектом передбачено розробка мережевого фільтру на базі одноплатного міні комп'ютера raspberry pi Основний вид роботи – це виконання монтажних робіт.

При виконанні монтажних робіт із прокладки мереж, працівник зіштовхується з небезпекою одержання різного роду травм, будь то механічні травми від обертових частин електроінструмента, электротравми від пробою ізоляції в електроінструменті або опіки від нагрітих у процесі роботи електроінструментів і продуктів їхньої обробки.

4.2 Розробка заходів з охорони праці

4.2.1 Виробничі приміщення

Під час планування будівлі варто врахувати три головні речі:

- місце знаходження сервера;
- місце знаходження маршрутизаторів;
- місце знаходження робочих місць співробітників.

З урахуванням цих пунктів і їх положення ми повинні побудувати мережу.

Місце знаходження сервера

Серверам виділяють окрему кімнату з хорошою вентиляцією і резервним живленням. Але в практиці сервер знаходиться в офісі адміністратора або адміністраторів які мають як і фізичний доступ до нього так і віддалений по мережі.

Варто приділити увагу на максимальну відстань тонкого клієнта від сервера ця довжина становить 35 метрів зв'язку фізичних обмежень кручений пари (патч корд). Це обмеження виправляється простою установкою репитера або додаткового маршрутизатора.

Відразу ж видно чому мережу тонких клієнтів варто планувати під час планування будівлі, це допомагає скоротити витрати на репітери і маршрутизатори. Кращий спосіб розміщення мережі це використовувати топологію "зірка" що дозволить ділити офіси і розширювати мережу.

Місце знаходження маршрутизатора

Ці пристрої відповідають за передачу інформації для тонких клієнтов.Которие дуже вразливі до енергійно перепадів і грозовим атакам. Варто приділити увагу на покупку маршрутизатора з урахуванням захисту від електричних перепадів.

Місце знаходження маршрутизатора повинно знаходитися далеко від співробітників і з резервним живленням. Кращі місце для нього може бути під стелею або в стінці в ящику ключ від якого може бути у адміністраторів.

Виділення окремого живлення потрібно для підтримки мережі під час критичних ситуацій.

Місце знаходження робочих місць співробітників

Ми вже уточнили що мережа буде розроблено з урахуванням топології "Зірка" так що розміщення робочих місць варто виділяти біля маршрутизатора що дасть можливість зручно встановити патч корди для тонких клієнтів.

Так само не варто забувати про резервне живлення що дасть можливість зберегти проекти під час перебоїв живлення.

4.2.2 Мікроклімат робочої зони працівників, вентиляція.

Згідно з ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень» встановлено норми допустимих параметрів мікроклімату для робіт в офісних приміщеннях (категорія робіт — легка 1а) :

- під час холодного періоду року температура повітря повинна бути не менше +21-25°С;
- температура поверхонь не менше + 19-24°С;
- відносна вологість повітря до 75%;
- зі швидкістю руху повітря 0,1 м / с.

А в літній сезон:

- температура приміщення повинна бути в межах + 22-28°С ;
- температура поверхонь не вище + 19-24°С,;
- відносна вологість повітря 40-60%;
- а швидкість руху повітря 0.1 м / с.

З таким мікрокліматом може стабільно працювати сервер та співробітники.

4.2.3 Безпека праці

При прокладці телекомунікацій в офісних приміщеннях монтажник виконує роботу як ручним, так й електроінструментом, а також працівник користується наступним інструментом: дриль, перфоратор, кутова шліфувальна машинка, шуруповерт.

При цьому мають місце шкідливі та небезпечні виробничі чинники, які можуть негативно діяти на працівника. До них відносяться:

- Роботи, виконувані електроінструментом:
- Перфорування отворів у бетонних і цегельних стінах.
- Штроблення каналів у бетонних і цегельних стінах.
- Обрізка кабельних каналів.
- Свердлення отворів у легких перегородках (гіпсокартон, ДСП).

- Загортання шурупів і гвинтів.

У перерахованого інструмента є обертові частини, які можуть нанести механічну травму. Крім того, при виконанні перерахованих вище робіт утворяться стружка, пил, осколки оброблюваної поверхні. Вони можуть поранити шкірні покриви, очі, дихальні шляхи. Також існує небезпека електротравм - як від пробою ізоляції в електроінструменті, так і при виникненні короткого замикання у випадку ушкодження схованої електропроводки. Не варто забувати про шуми й вібрацію, які супроводжують роботі даним інструментом. При роботі електроінструмент і продукти його обробки можуть нагріватися й, отже існує небезпека термічних травм (опіків).

- Роботи, виконувані ручним інструментом:
- Забивання в отвори пластикових пробок і дюбелів.
- Обрізка кабелю.
- Зачищення кабелю від ізоляції.
- Обтиск проводів у технологічні клеми.

При виконанні даних робіт монтажник користується наступним ручним інструментом: викрутка, молоток, пассатіжи, гострозубці, бокорізи, пристосування для зачищення й обрізки кабелю. У перерахованого інструмента є гострі ріжучі крайки, об які можна порізатися.

4.2.4 Загальні вимоги щодо охорони праці при роботі з інструментом та пристроями

Правила з охорони праці під час роботи з інструментом та пристроями встановлюють державні нормативні вимоги з охорони праці під час роботи з інструментом та пристроями. Правила обов'язкові для виконання роботодавцями - юридичними та фізичними особами незалежно від їх організаційно-правових форм та форм власності, які здійснюють роботи з використанням інструменту та пристроїв, за винятком роботодавців - фізичних осіб, які не є індивідуальними підприємцями.

На основі Правил розробляються інструкції з охорони праці для професій

та видів робіт.

Перед виконанням роботи із застосуванням інструменту та пристосувань працівник повинен провести візуальний огляд всього використовуваного інструменту та пристроїв щодо наявності пошкоджень та виявлення їх несправності. Працювати з несправним інструментом та пристроями забороняється.

При роботі з інструментом та пристроями працівник зобов'язаний) застосовувати засоби індивідуального захисту, виконувати тільки ту роботу, яка доручена керівником роботи та за виконанням якої працівник пройшов інструктаж з охорони праці, працювати тільки з тим інструментом та пристроями, при роботі з якими працівник навчався безпечним методам та прийомам виконання робіт.

4.2.5 Електробезпека

Електричні установки, до яких відноситься практично вся офісна оргтехніка, надає для людини можливу небезпеку. Оскільки в процесі експлуатації або проведення профілактичних робіт, людина може торкнутися частин, що перебувають під напругою.

Умови електробезпечності залежать і від параметрів навколишнього середовища виробничих приміщень - вологість, температура й т.д Для попередження поразки електричним токовищем при експлуатації електроустановок використають технічні засоби захисту, до яких відносять:

- електричну ізоляцію струмоведучих частин,
- захисне заземлення,
- занулення,
- вирівнювання потенціалів,
- захисне відключення,
- електричний поділ мережі,
- мала напруга,
- подвійну ізоляцію.

Експлуатація комп'ютерної мережі передбачає використання ПК в якості пристроїв доступу до неї. Джерелом напруги живлення ПК і Wi-Fi-роутерів є мережа змінного струму з напругою 220 В, на яку поширюється ГОСТ 25861-83.

Згідно з вимогами для попередження уражень струмом необхідно:

- чітко і в повному обсязі виконувати правила виконання робіт і правила технічної експлуатації;
- виключити можливість доступу оператора до частин обладнання, що працює під небезпечною напругою, неізольованих частин, призначеним для роботи при малому напрузі і не підключеним до захисного заземлення;
- застосовувати ізоляцію, служить для захисту від ураження електричним струмом, виконану із застосуванням міцного суцільного або багатошарового ізоляційного матеріалу, товщина якого обумовлена типом забезпечується захисту;
- підводити електроживлення до ПК від розетки будівлі за допомогою спеціальної вилки з занулюючих контактом;
- надійно підключити до заземлюючих затискачів металеві частини, доступні для оператора, які в результаті пошкодження ізоляції можуть опинитися під небезпечною напругою;
- перевірити, що захисний заземлювальний провідник не має вимикачів і запобіжників, а також надійно ізольований.

4.3 Пожежна безпека

Для розміщення первинних засобів пожежогасіння у виробничих, складських, допоміжних приміщеннях, будівлях, спорудах, а також на території підприємств, як правило, повинні встановлюватися спеціальні пожежні щити (стенди). На пожежних щитах (стендах) повинні розміщуватися ті первинні засоби пожежогасіння, які можуть застосовуватися в даному приміщенні, споруді, установці.

На пожежних щитах (стендах) необхідно вказувати їх порядкові номери

та номер телефону для виклику пожежної охорони.

щити (стенди) повинні забезпечувати:

- захист вогнегасників від потрапляння прямих сонячних променів, а також захист знімних комплектуючих виробів від використання сторонніми особами не за призначенням (для щитів та стендів, установлюваних поза приміщеннями);
- зручність та оперативність зняття (витягання) закріплених на щиті (стенді) комплектуючих виробів.

Вибір типу та необхідна кількість вогнегасників визначається відповідно до Типових норм належності вогнегасників, затверджених наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 02.04.2004 N 151 та зареєстрованих в Міністерстві юстиції України 29.04.2004 за N 554 / 9153.

Пожежні щити (стенди), інвентар, інструмент, вогнегасники в місцях установлення не повинні створювати перешкоди під час евакуації.

Вогнегасники, встановлені за межами приміщень або в неопалюваних приміщеннях та не призначені для експлуатації при мінусових температурах, повинні зніматися на холодний період. В такому випадку на пожежних щитах та стендах повинна розміщуватися інформація про місце розташування найближчого вогнегасника.

ВИСНОВКИ

У дипломній роботі було проведено аналіз та розробку мережевого фільтра на базі raspberry pi, що використовує набір доступних та безкоштовних інструментів для фільтрації мережевого трафіку, що проходить через маршрутизатор.

Використовуючи цю розробку з мінімальними вкладеннями людина може забезпечити свою мережу відмінним щитом, що блокує мережеві загрози, сміттєві банери та будь-якого роду рекламу.

У першій частині диплома було зроблено аналіз існуючих моделей raspberry pi. Raspberry pi zero маючи ряд переваг поступається молодішим версіям через присутність пару рядів переваг, а саме наявність просунутого мережевого контролера, вилученого процесора, наявність графічного процесора, присутність usb 3.0 та інші переваги описані в першій частині.

Але відсутність всього цього не заважає створити мережевий фільтр, звичайно у вас не завантажуватимуться blu ray фільми за кілька миттєвостей і ви не зможете використовувати модель zero у великих офісах через перевантаження слабкого фільтра АЛЕ для домашньої мережі його вистачить за очі.

У другій частині диплома йде реалізація мережевого фільтра. Покрокова інструкція дозволяє створити власний блокувальник реклами використовуючи raspberry pi zero за 5$ та набір безкоштовних інструментів.

Починаючи з установки Raspberry Pi OS людина вже отримує уявлення про рівень складності реалізації проекту, але використовуючи даний дипломний проект будь-який користувач зможе зробити установку raspbian на sd карту, подальшу установку на окремий том і установку та настроювання інструментів. Цими інструментами є PI HOLE та PI VPN присутність другого необов'язково, але як частина канонічного мережевого фільтра було встановлено та налаштовано у цьому проекті.

PI HOLE має у собі базу даних рекламних ресурсів, а маючи базу з DNS

рекламами нескладно розпочати їх фільтрацію з мережі. **PI VPN** дає можливість створити мережевий "тунель", що дозволяє приховати свій мережевий трафік від очей провайдера.

У третій частині диплома були проведені тести мережевого фільтра використовуючи віртуальну машину з Windows OS, а також надання інформації вже виправленої вразливості. На скріншотах можна було побачити, що мережевий фільтр особливо не знизив швидкість з'єднання машини з провайдером.

У четверній частині розповідається про техніку безпеки установки мережевого фільтра в офіс і про умови клімату, в якому повинен перебувати raspberry pi.

У загальних підсумках мережевий фільтр необхідний щоб захиститься від головної вразливості будь-якого комп'ютера, сервера і телефону. А головною вразливістю є не грамотний та не підкований користувач цих пристроїв.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ІНФОРМАЦІЇ

1. Mulcas.com: [Електронне джерело] - Установки на vmWare;

URL - https://mulcas.com/raspberry-pi-os-in-a-virtual-machine-with-vmware/

2. Currentware: [Електронне джерело] - Види мережевих фільтрів;

URL - https://www.currentware.com/blog/web-content-filtering/

3. Webtitan: [Електронне джерело] - Технології мережевого фільтра;

URL - https://www.webtitan.com/network-web-filter/

4. W3schools: [Електронне джерело] - Мережеві протоколи;

URL - https://www.w3schools.in/types-of-network-protocols-and-their-uses

5. Currentware: [Електронне джерело] - Мережевий фільтр у навчальному закладі;

URL - https://www.currentware.com/blog/should-schools-use-content-filtering-software/

6. Tomshardware: [Електронне джерело] – Вибір raspberry pi;

URL - https://www.tomshardware.com/how-to/raspberry-pi-buying-guide

7. Github: [Електронне джерело] – Вразливості raspberry pi;

URL - https://n4nj0.github.io/advisories/pi-hole-multiple-vulnerabilities-i/