Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
(повна назва інституту/факультету)

Кафедра телекомунікацій
(повна назва кафедри)

«На правах рукопису»
УДК _____

До захисту допущено
Завідувач кафедри

_____ Сергій КРАВЧУК
(підпис) (Ім'я, прізвище)

"___"_____2020_р.

Магістерська дисертація

на здобуття освітнього ступеня «магістр»

Спеціальність172 Телекомунікації та радіотехніка,
(код і назва)

За освітньо-професійною програмою Інженерія та програмування інфокомунікацій.

на тему:«Можливості хакерських атак в телекомунікаційних мережах» ____

Виконав: студент 2курсу, групи ТЗ -91мп
(шифр групи)

Середюк Дмитро Олександрович_____ _____
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник с.н.с. к.т.н., доц. каф. ТК Міночкін Д.А.____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант_____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент_____с.н.с. д.т.н., проф. каф. ІТМ Скулиш М.А. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2020 рік

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем
(повна назва)

Кафедра телекомунікацій
(повна назва)

Спеціальність 172 Телекомунікації та радіотехніка
(код і назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою Інженерія та програмування інфокомунікацій.

ЗАТВЕРДЖУЮ
В.о.завідувача кафедри

_____Явіся В.С.
(підпис) (ініціали, прізвище)

«20 »січня2020 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Середюк Дмитро Олександрович
(прізвище, ім'я, по батькові)

1. Тема дисертації :«Можливості хакерських атак в телекомунікаційних мережах»

науковий керівник дисертації к.т.н.,доцент. каф. телекомунікацій Міночкін Д.А.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від «03»« листопада » 2020 р. № 3208-с

2. Строк подання студентом дисертації12.12.2020

3. Об'єкт дослідження кібератака на телекомунікаційну мережу та її захист.

4. Предмет дослідження кібератака з застосуванням методів масового нападу на основі існуючих концепцій та захисту від них.

5. Перелік завдань, які потрібно розробити

1) Виконати огляд літератури з теми дослідження. Розглянути поняття Кібератака та кібербезпека, дослідити основні сфери;

2) Розглянути існуючі методи атаки та захисту на телекомунікаційні мережі;

3) Виконати розробку технічного рішення від кібератаки.

6. Орієнтовний перелік ілюстративного матеріалу структурна схема високопродуктивної оболонки для захисту від кібератак для телекомунікаційної мережі; методологія атак; результати оцінки кібератак; результати оцінки кіберзахисту.

7. Орієнтовний перелік публікацій

1) Свідоцтво про реєстрацію авторського права на твір №79688, Науковий твір: «Методологія захисту персональних даних в Wi-Fi мережах»

(Додаток 1)

2) Свідоцтво про реєстрацію авторського права на твір №76226, Науковий твір: «Модель проектування бездротової мережі Wi-Fi на основі стандарту 802.11»

(Додаток 2)

3) Свідоцтво про реєстрацію авторського права на твір №76224, Науковий твір: «Декомпозиція методів захисту мережі передачі даних від перевантажень»

(Додаток 3)

4) Свідоцтво про реєстрацію авторського права на твір №76225, Науковий твір: «Методика оцінювання систем підтримки мобільності для мереж 4-го покоління з малими стільниками»

(Додаток 4)

5) Свідоцтво про реєстрацію авторського права на твір №76214, Науковий твір: «Трансляція радіосигналів цифрового телебачення стандарту DVB-C по наземному радіоканалу НВЧ-діапазону»

(Додаток 5)

6) Свідоцтво про реєстрацію авторського права на твір №76223, Науковий твір: «Метод оптимізації антені супутникового ретранслятора для досягнення умов узгодження координації з іноземними адміністраціями» (Додаток 6)

8. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання 28.10.2019

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Підбір літератури з теми дослідження	01.11.2019 - 09.06.2020	виконано
2	Пошук інформації про існуючі стандарти, їх можливості та недоліки	01.12.2019 - 15.12.2019	виконано
3	Побудова тестової мережі для випробувань	02.04.2020 -16.04.2020	виконано
4	Написання розділу: Аналіз підходів для атаки та захисту телекомунікаційних мереж	10.06.2020 – 20.07.2020	виконано
5	Написання розділу: Аналіз атак та високопродуктивні рішення кібератак на телекомунікаційні мережі	21.07.2020 – 25.08.2020	виконано
6	Написання розділу: Методи побудови кіберзахисту телекомунікаційних мереж	26.08.2020 – 17.10.2020	виконано
7	Написання розділу: Загальні технічні рекомендації	18.10.2020 – 02.12.2020	виконано
8	Оформлення магістерської дисертації	03.12.2020 – 12.12.2020	виконано

Студент _____ Середюк Д.А.
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Міночкін Д.А.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Робота містить 84 сторінки, 23 рисунки. Було використано 35 джерел.

Мета роботи: розробити методики захисту від найпоширеніших кібератак на основі існуючих методик захисту

Об'єкт дослідження: кібератака на телекомунікаційну мережу з її захистом.

Предмет дослідження: кібератака з застосуванням методик масового нападу на основі існуючих концепцій та захисту від них.

В представленій роботі розглянута концепція, як хакери думають і діють, основні вказівки щодо підходу до кібербезпеки та захисту від найбільш поширених кібератак. Дане дослідження проводиться навколо типової діяльності та встановлення телекомунікаційних мереж, додатків Інтернету або веб-сайтів, які містяться в цьому додатку. Спочатку будуть пояснені закони та методологія хакера. Використовуючи елементи з цієї частини,далі буде представлений перелік поширених атак із їх конкретними рішеннями, щоб уникнути їх зіткнення.

Ключові слова: кібер-атака-безпека, хакерство, вразливість та безпека.

ABSTRACT

The work contains 84 pages, 23 figures. 35 sources were used.

Purpose: Develop defense techniques for the most widespread cyber attacks on the basis of existing defense techniques

Object of research: Cyber attack on the telecommunications network with its protection.

Subject of research: Cyberattack with the use of methods of mass attack on the basis of existing concepts and protection against them.

This paper examines the concept of how hackers think and act, the basic guidelines on how to approach cyber security and protection against the most widespread cyber attacks. This study is conducted on typical activities and installation of telecommunication networks, Internet add-ons or Web sites that reside in this add-on. First, the laws and methodology of the hacker will be explained. Using the elements of this section, we will present a list of common attacks with their specific solutions to prevent them from happening.

Keywords: cyber-attack-security, hacking, vulnerability and security.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

Active Directory- Служба каталогів Microsoft, яка дозволяє адміністраторам управляти цілою телекомунікаційною системою

API “Інтерфейс програмування програм”

Backdoor видає хакерський доступ до комп’ютера мережі.

Bruteforce Метод злому, що використовується для паролів, які складається із складання відгадок до відгадування

Cookie містить налаштування користувача або інформацію про веб-сайт

Denial of Service (DoS) Атака відмови в обслуговуванні (DoS), яка полягає в тимчасовій нейтралізації послуги , тобто багато запитів

DNS "Система доменних імен", перекладає IP адреси в доменні імена та навпаки

GPO “Об’єкт групової політики”, особливість Active. Скорочення зловмисного програмного забезпечення “шкідливого програмного забезпечення”

Malware перехоплення кожного зв’язоку між двома машинами

Privilege escalation Набір дій, які дозволяють простому користувачеві мати права адміністратора

Ransomware (вірус Хімера, Петя) Вимірювальне програмне забезпечення, яке шифрує файли з комп’ютера і вимагає викуп, у порядку, отримати ключ для їх розблокування

Script kiddie погана кібербезпека, хакер намагається проникнути в систему використовуючи вже виготовлені інструменти

Sniffer Програмне або апаратне забезпечення, яке перехоплює дані з мережі та аналізує їх

Virus шкідливе програмне забезпечення, яке копіюється та поширюється на інші комп'ютери. Збиток може бути серйозним, як знищення файлу так і відмова у сервісі

Worm Подібно до вірусів, хробаки є самостійними програмними забезпеченнями та поширюється без допомоги людини

Zero-day vulnerability Уразливість, якої ще не було виявлено та не виправлено

ВСТУП

Поряд із вигодами, які приніс підйом Інтернету та мережевих технологій постає нова проблема. Сфери, які постраждали від злочинності, зростали, як загально відомо в телекомунікаційних мережах, веб-сайти та бази даних було дедалі ширшими, і люди незабаром зрозуміли що їх талант у роботі з комп'ютерами можна використовувати для здійснення зловмисних операцій. Пошук шляхів щоб зловживати телекомунікаційними системами та мати доступ до розкритої інформації, стало загрозою для всього інтернету.

Після визначення кібербезпеки та злочинності ця магістерська робота буде зосереджена на хакерській методології. Розуміння, яка мета цих людей і як вони поступають коли вони хочуть здійснити наступальний маневр – це головна перевага. Беручи відомі нотатки загальних закономірностей, мережа може поставити себе на захист від хакера і передбачити напади. Рішення деяких існуючих кібератак будуть наведені в цій магістерській роботі,
разом з іншими рекомендаціями, від експертів з кібербезпеки. Порада про стратегії щодо мереж та управління веб-послугами буде нарешті представлена.

Особлива увага булла приділена законодавчим актам, і жодної дії в цій роботі не було здійснено незаконно. Кожна зловмисна команда запускалася проти добровільно вразливої віртуальної машини з іншої віртуальної машини, обидва перебуваючи в одній приватній телекомунікаційній мережі.

Дуже часто телекомунікаційні системи схильні недооцінювати важливість кібербезпеки та безпеки від кібератак. Насамперед такі системи дорогі або занадто складні, заходи з кібербезпеки іноді ігноруються, а деякі телекомунікаційні системи виявляються відкрито вразливими для будь-якого

хакера, який хотів би цим скористатися. Атака може бути дуже сильною в залежності від сфери діяльності.

Ця магістерська робота спрямована на те, щоб допомогти телекомунікаційним системам та мережам зрозуміти, як хакери думають і діють, і що дають їм основні вказівки щодо підходу до кібербезпеки та захисту від найбільш поширених кібератак, що трапляються на сьогодні.

Дослідження проводиться навколо типової

Діяльності телекомунікаційних систем, що означає інформацію, яка стосується внутрішніх мереж, Інтернету, чи веб-сайтів, які містяться в цій роботі.

В дані магістерській роботі будуть пояснені типові помилки, а також інструменти та методи представлені відповідно до отриманих відповідей, а також документації від спеціалізованих компанії.

Спочатку будуть пояснені закони та методологія хакера. Використовуючи елементи з цієї частини,

Плавно приведуть до переліку поширених атак із їх конкретними рішеннями, щоб обійти зіткнення з ними.

Нарешті рішення, включаючи процеси, найкращі практики, технологічні заходи та інструменти будуть обговорюватися далі.

За результатами роботи буде показано, що навіть маючи низький бюджет, телекомунікаційні мережі можуть захиститися від атаки, що трапляється на сьогодні. Є багато елементів, які можна реалізувати, що сприятиме рівню безпеки, а також підготувати телекомунікаційну систему до реагування на сучасні кіберзагрози. Навіть якщо загальну безпеку неможливо налаштувати, дана робота дає хороший огляд того, на чому слід зосередитись і як себе захистити.

1 АНАЛІЗ ПІДХОДІВ ДЛЯ АТАКИ ТА ЗАХИСТУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

1.1 Сфера застосування

Багато речей піддані Інтернету і, можливо, вразливі до кібератаки. Оскільки ця магістерська робота зосереджена на телекомунікаційні мережі підприємницької діяльності то буде описано про вразливі місця, які можна знайти в апаратному та програмному забезпеченні, які в компанії сприйнятливі, наприклад, сервери, внутрішні телекомунікаційні мережі тощо. Перелік усіх вразливих місць буде занадто довгим, тому в ці магістерські роботі буде взято до уваги лише найпоширеніші та найважливіші слабкі місця і зупинитися на моментах успішної атаки. Багато аспектів кібербезпеки були виключені із сфери застосування. Перший є мобільний злом. Хоча провідні атаки, спрямовані на мобільний телефон, можуть скомпрометувати безпеку телекомунікаційної мережі, якщо на ній зберігається конфіденційна інформація, це вважається непрямою атакою. Це також передбачається, що у всьому документі хакер не має доступу до фізичних ресурсів телекомунікаційної мережі, тому всі методи злому, що включають маніпуляції з апаратним забезпечення залишаються осторонь. Нарешті, системи домашньої автоматизації злом та експлуатація вразливості інших телекомунікаційних систем охоче не включаються.

1.2 Важливість кібербезпеки

Кібербезпека, як і всі види безпеки, спрямована на захист конфедеційних даних. У цьому випадку критичними ресурсами є комп’ютери, маршрутизатори, телекомунікаційні мережі або хмара, і вони мають вирішальне значення для належного функціонування. Безсумнівно коли знання про комп’ютери чи інтернет-протоколи були не такими прогресивними, як сьогодні, кібербезпека не обмежується лише технічними

заходами. Насправді, кібербезпека - це термін, який охоплює не лише телекомунікаційні технології, а й бізнес процесів та людей.

Всі заходи безпеки спрямовані на те, щоб допомогти захистити себе від загроз, слід важати що є 3 компоненти кібербезпеки. Перший компонент - це конфіденційність, яка охоплює всі засоби контролю, які можуть мати доступ до конфіденційних даних, таких як аутентифікація або шифрування. Другий це цілісність, яка спрямована на збереження достовірності інформації. Насправді, конфіденційні дані не повинні змінюватися користувачами, які не мають на це прав, а також технічні проблеми як збої системи. Третій і останній компонент - це доступність і надійність надання уповноваженим користувачам доступу до конфіденційної інформації. Сюди входить оновлення системи, коли це можливо, і мають заходи відновлення, такі як плани резервного копіювання та резервування.

Однак кібербезпека не повинна бути перешкодою та ускладнювати роботу працівників. Зробити процеси довшими та менш зручними для користувача заради безпеки рішення, яке необхідно вивчити. В результаті буде реалізовано більше функціональних можливостей у програмі в інших заходах безпеки. Кожне рішення матиме вплив на один-на одного.

1.3 Кіберзлочинність

За визначенням, кіберзлочинець - це «особа, яка вчиняє кіберзлочини там, де вона / він використовує комп’ютер або як інструмент, або як ціль, або як те і інше ». Тут ми можемо знайти поняття телекомунікаційної технології та поняття злочину. Останній більш складний у визначенні та варіюється залежно від країни, отже і різні закони, які існують. Навколо, це можна підсумувати, охоче завдаючи шкоди фізичній особі чикомпанії шляхом доступу, модифікації або видалення секретної інформації. Це може приймати багато форм та форми, а деякі будуть описані в цій магістерській роботі.

1.3.1 Мотивація зловмисників

Хакерів може бути кілька типів, що мають кілька цілей. Перший і найнебезпечніший один - часто шукає фінансовий прибуток, цей профіль хакера може вирішити і напасти на організацію лише заради цього, оскільки робити щось незаконне є для них не проблема. Вони потенційно можуть завдати великих збитків і викрасти важливі дані, які будуть продаватися в темній мережі або використовується для компрометації інших компаній. Другий тип хакерів - це особи, які мають дозвіл на компрометацію системи. Також називаються етичними хакерами, їх метою є допомогти компанії знайти вади в своїй системі, не зловмисно, а експлуатуючи їх.
Третій тип хакерів - це дещо і те, і інше. Вони знаходять уразливі місця та настороженість адміністраторів, але їх діяльність з виявлення порушень є незаконною.

Найчастіше гроші або важливі документи є основними причинами, чому кіберзлочинці вирішують зламати дану телекомунікаційну мережу, тому банки, повинні усвідомлювати, що їх бізнес – це головна ціль і відповідно планувати свою безпеку.

Хакер, який бореться за своє переконання називають хактивістом, і він може стати небезпечним, якщо утворе свою.
Нарешті, хакери можуть перегрупуватися, щоб здійснити найскладнішу форму кіберзлочинності: розширена стійка загроза (РСЗ). Головна мета - викрасти конфіденційні дані, тому урядові або дійсно важливі компанії, найімовірніше, будуть націлені. Значення використовуються різноманітні, і все організовано, що показує, що люди організовують
атаку професіоналами. Їх мета не знищити, а проникнути в систему і залишатися якомога довше, не виявившись.

1.3.2 Огляд ризиків

Зловмисники можуть скористатися багатьма наявними шкідливими

програмами, що призводять до різних сценаріїв. Основні віруси або хробаки не завжди вимагають віддаленого доступу до комп’ютера чи телекому - нікаційної мережі і можуть бути надіслані електронною поштою. Але коли зловмисник має віддалений доступ до комп'ютера, він у своєму розпорядженні безліччю дій та шкідливих інструментів.

Окрім отримання конфіденційної інформації для телекомунікаційних систем, він може залишити задні двері для легкого підтримування свого доступу до вразливого комп'ютера чи телекомунікаційного сервера. Він може отримати пароль, пов’язаний з файли, використовувати інструменти, щоб зламати їх і порушити облікові дані кожного облікового запису. Кейлоггери також можна використовувати для збору кожної клавіші, яку жертва натискає на своїй клавіатурі, і надсилання їх до зловмисника. Йдучи ще далі, хакер може виконати атаку "посередині" і перехоплювати кожен зв’язок, який надсилається між комп’ютерами чи між телекомунікаційними системами. Можливості величезні а злочинці, які знають, що роблять, можуть завдати непоправної шкоди телекомунікаційній системі. Ось чому кібербезпеку не слід недооцінювати, а як активну позицію потрібно приймати, щоб уникнути таких ситуацій, коли доля телекомунікаційної системи залежить від неї.

1.4 Законодавство та правові норми ЄС

Навіть якщо деякі країни мають закони, характерні норми для кіберзлочинності, або пристосували свої правові норми, часто важко знати, який із них застосувати, оскільки Інтернет не має кордонів і порушення не пов'язане з фізичним місцем знаходження. Насправді, маючи спеціальний суд з питань кіберзлочинів мало б сенс, але сьогодні нічого як такого не існує (Simons, 2018).

У Європі Агентством Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) є головне агентство експертів з кібербезпеки, створене в 2004 році. Це спрямоване на допомогу країнам, що знаходяться

всередині ЄС для вирішення проблем кібербезпеки, але також публікує дослідження та різні звіти та правові норми. Також слід відзначити в Директиві про СНД (Директива про Мережеві та інформаційні системи), що є першим законодавством, створеним у 2016 році, метою якого є підготовка країн для майбутніх кібератак, вимагаючи від компетентного органу на національному рівні, щоб створити групу співпраці для обміну інформацією та, як правило, покращення кібербезпеки ефективністю та потужністю. Тоді члени ЄС мали можливість пристосуватись до 9 травня 2018 року їх національне законодавство, що визнає цю директиву (Директива про безпеку мережі та інформаційні системи, 2018).

Загальне положення про захист даних від квітня 2016 року застосовується з 25 травня2018. Це має наслідки для різноманітних телекомунікаційних систем не лише з Європейського Союзу, але і ззовні. Як тільки дані резидента ЄС зберігаються або обробляються в Європі, це підпадає під дію цього закону. Тепер у в телекомунікаційних системах повинно бути причини зберігати сприйнятливу інформацію та ідентифікувати особу, таку як ім’я, електронну адресу чи навіть дані про місцезнаходження, та мати згоду цієї особи, яка може в будь-який момент запитати, про дані які зберігають для них, і якщо вони бажають, попросити видалити всю інформацію, що стосується них (ст. 4 GDPR Визначення).

Що стосується кібербезпеки, компанії повинні діяти відповідно до даних. Стаття 25 під назвою "Захист даних за проектом і за замовчуванням", вказує, що контролер, такий як особа або державна установа повинні “впроваджувати відповідні технічні та організаційні заходи ефективно "(ст. 25 GDPR Захист даних за проектом та за за замовчуванням). Це передбачає реструктуризацію та ефективну роботу компаній щодо дотримання відповідно до цих стандартів, щоб обмежити можливість порушення та відповісти, якщо кібератака або випадковий витік, що компрометує дані клієнтів. Якщо так, то телекомунікаційна система повина повідомити в

наглядовий орган протягом 72 годин після виявлення порушення. Компанії та телекомунікаційні системи певного підприємства, які вирішили не дотримуватись GDPR, стикаються з цим, залежно від порушеного статей, штраф у розмірі 20 мільйонів євро або 4% їх річного доходу.

2 АНАЛІЗ АТАК ТА ВИСОКОПРОДУКТИВНІ РІШЕННЯ КІБЕРАТАК НА ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ

2.1 Основні кроки кібер атаки

Досвідчений хакер не буде продовжувати атакувати телекомунікаційну систему, не знаючи, на що вона здатна. Він проходить різні етапи, щоб визначити, яку архітектуру використовує ціль, яку порти нього можуть виставити безпеку чи з чого почати пошук вразливостей. Ці попередні кроки розділені на 3 методи.

2.2 Метод «Слід»

Першим кроком, який потрібно зробити перед нападом, є збір інформації про жертву. Чим більше злочинець знає про використовувані телекомунікаційні технології, тим більше кутів атаки він, можливо, має. Цей перший обов'язок полягає в тому, щоб знати, яку структуру може мати компанія чи взагалі мати уяву про загальну телекомунікаційну систему яка використовується. Для цього існують різні інструменти та техніка, і на даний момент навиків майже немає. Деякі телекомунікаційні системи та мережі компаній чи підприємств, як правило, надають занадто багато інформації на своєму веб-сайті або в соціальних мережах. Якщо конфігурації сервера доступна безпосередньо для всіх, це означає полегшення та можливий напад. За лічені хвилини винахідливий хакер може зрозуміти, чи це саме так система сприйнятлива до уразливостей. Також коментарі, залишені у файлах HTML файлу веб-сайт може іноді видавати критично важливі дані зловмиснику. Будь-яка конфігурація, електронна пошта, адреси чи імена беруться до уваги злочинцем, оскільки він міг би знайти для них користь.

Для цього майже не потрібно ніяких зусиль, це так достатньо лише для того, щоб знати, як шукати інформацію за допомогою пошукових систем. Зловмисник може використовувати деякі команди або програмне забезпечення для отримання інформації, яка є також цінною: IP-адреси. "Whois" - це команда, яка запускається в Unix або Windows також доступний в Інтернеті. Він запитує DNS, щоб повернути IP-адреси та інформацію про власника веб-сайту. За допомогою команди “ping” на веб-сайті можна також виявити його IP-адресу.

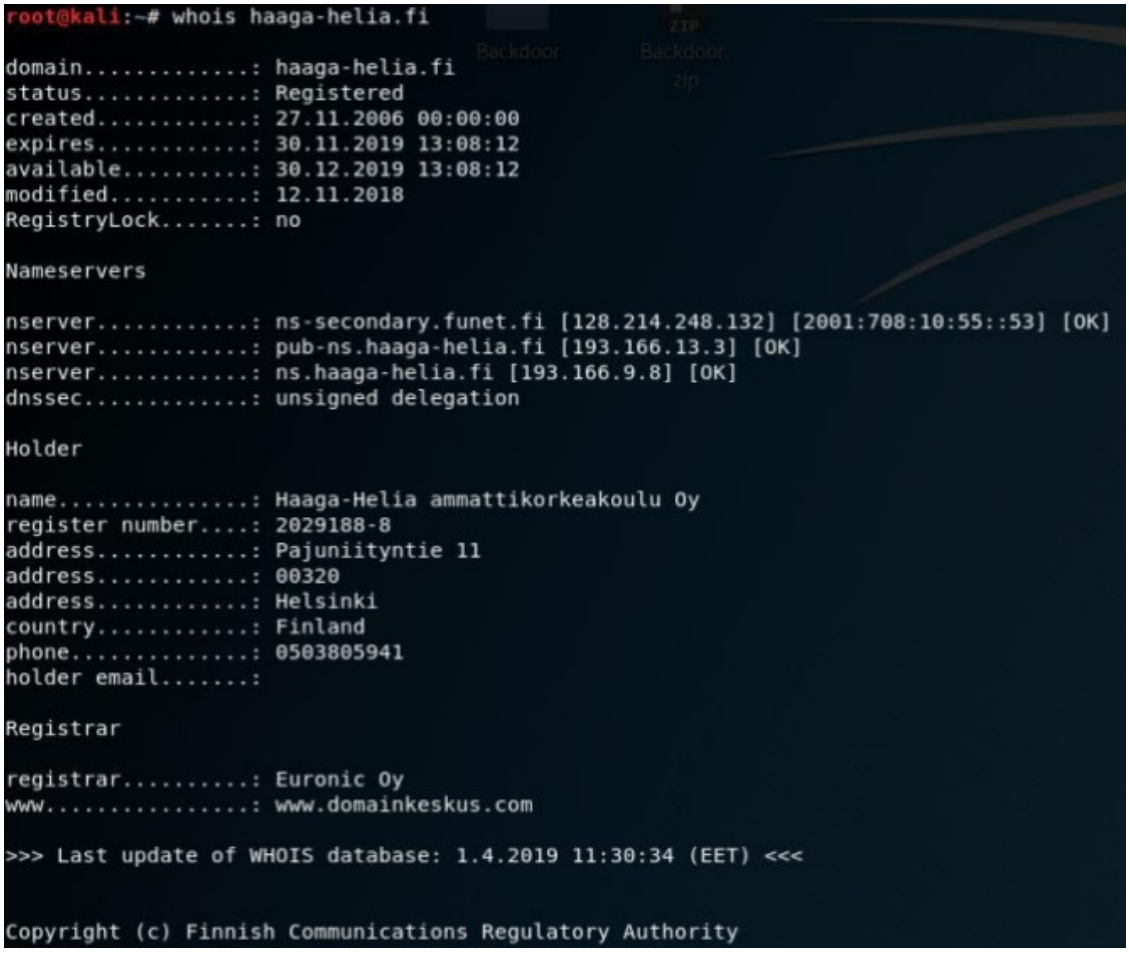


Рисунок 1 Команда “who is”

Іншу цінну інформацію можна отримати за допомогою команд. "Дмитро" - це пакет, який дозволяє користувачеві робити запити “who is” та різні операції. Серед інших, “- параметр winse ”дає нам більше подробиць про адресу та хост.

Існує багато інструментів, які можуть допомогти зловмиснику отримати інформацію про Інформаційну телекомунікаційну систему. Основна мета - ознайомитись із телекомунікаційною мережею та Послугами які вона надає, якомога більше використовуючи як легальні, так і нелегальні методи.

2.3 Метод «Сканування»

Метод полягає у скануванні телекомунікаційних систем, щоб побачити, які порти відкриті чи які служби працюють. На продовженні попереднього методу цілей стає більше та точнішими уразливі місця. Тоді як операції по відбитку можна робити повністю анонімно та без проблем, сканування вимагає трохи більшої обережності, оскільки деякі дії можуть реєструватися на атакованому сервер або виявлятися як підозріла діяльність системами виявлення вторгнень.

Найвідомішим інструментом для цього є "nmap". Це універсальний інструмент, який дозволяє користувачеві відкривати хости та служби в мережі (Nmap Introduction, 2019). Команда, доступна як на Windows так і Unix, містить величезну кількість параметрів, найцікавішими з яких є такі, що дозволяють сканувати без загрози бути виявленим. Це робиться, не заповнюючи Тристороннє підключення, надіславши пакет скидання (RST) після відповіді від сервера виявляючи, що порт відкритий.

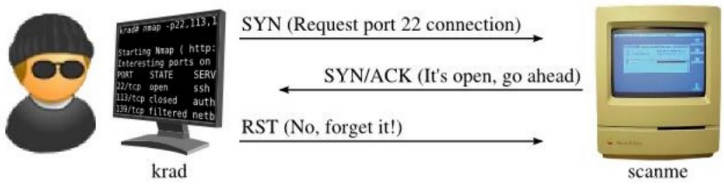


Рисунок 2 Тристороннє підключення, перерване пакетом RST (Nmap Network Scanning)

Даний метод не обходиться без недоліків, оскільки ці сканування все ще можна виявити в журналі, а тому, що велика кількість пакетів RST може виглядати підозріло. Щоб бути ще безпечніше, “nmap” пропонує можливість затримки сканування для зменшення впливу вторгнення в телекомунікаційну систему (сканування телекомунікаційної мережі Nmap).

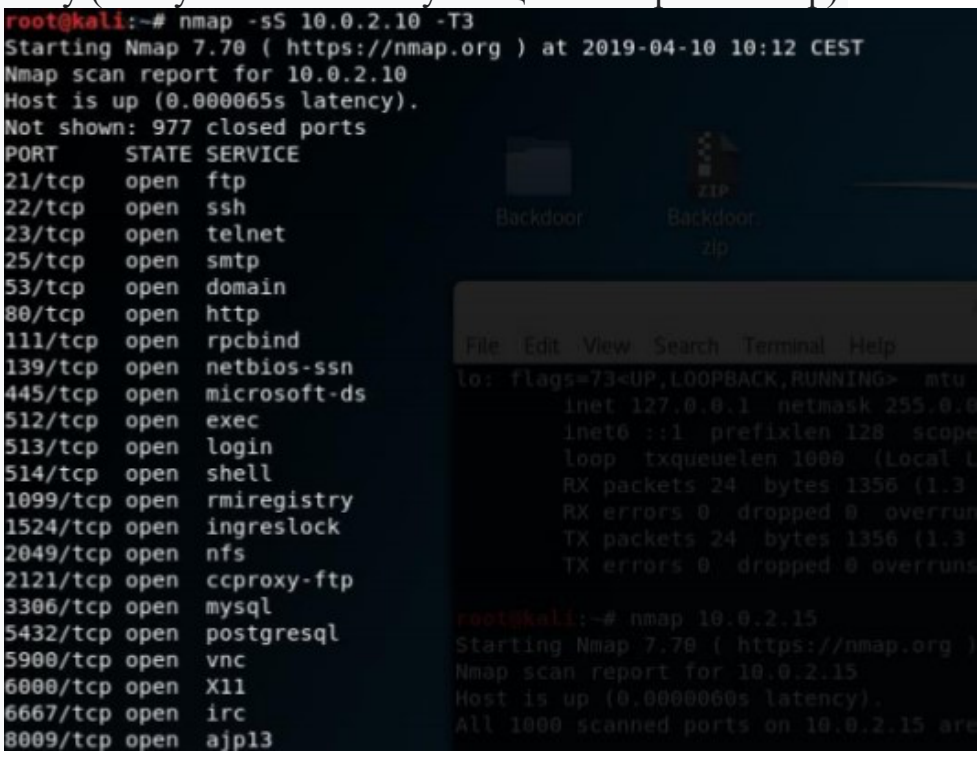


Рисунок 3 Тихе сканування портів з нормальним часом затримки (Ч3) “nmap”

“Netcat” - це також хороший інструмент для сканування відкритих портів, що пропонує безліч можливостей для встановлення з'єднання, але також з можливістю залишити задні двері.

2.4 Метод «перерахування»

Наступний заключний метод складається з того, щоб мати найбільш точне уявлення про те, з чого зроблена певна телекомунікаційна система тобто вибрана ціль. Використовуючи "netcat", "nmap" або інші стратегії, мета полягає в тому, щоб мати тип послуги, який є запущеним та його версію. Дані, отримані з DNS-серверів, можна отримати шляхом запиту Сам DNS. Найкращим сценарієм для зловмисника буде те, що дозволені передачею зони. Передачею зони означає, що хакер видає себе за підлеглого DNS і запитує основний DNS-сервер для отримання інформації про весь список імен хостів. Якщо це вдасться, можна отримати вичерпне перерахування субдоменів та їх IP-адреси. Іншим рішенням для отримання списку субдоменів є використання грубої сили та перевірка власноруч, чи є кожен запис дійсним. Ця операція можлива, що і є сценарієм тобто відсканований запис DNS після спроби виконати передачу зони DNS.

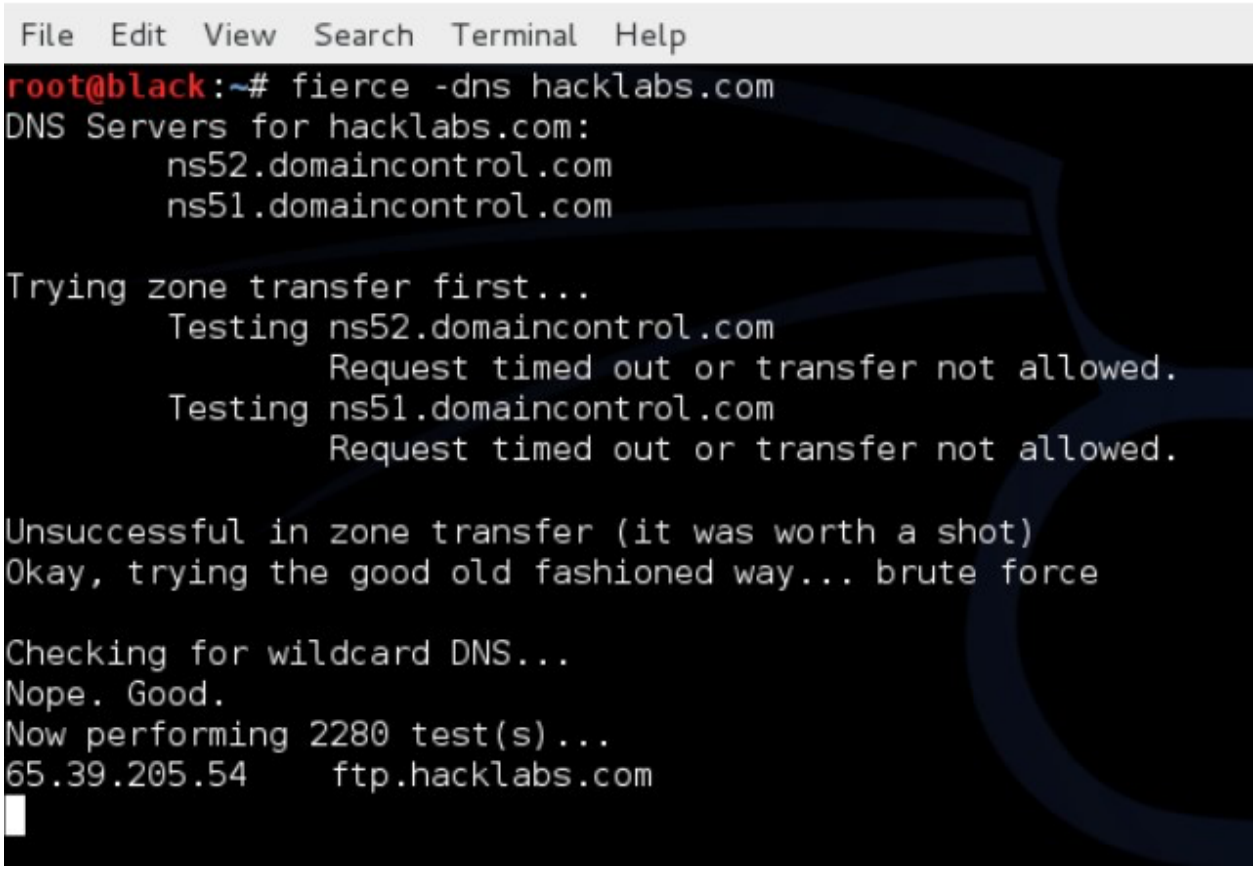


Рисунок 4 Пошук субдоменів

Також можна отримати інформацію про інші служби, окрім DNS. Зловмисник може дивитись назви служби та версії, а потім шукати потенційні уразливості місця в телекомунікаційній мережі.
Цей процес називається захопленням банера, доречі існує декілька способів. HTTP-сервери, SSH або FTP-сервери піддаються данному ризику.

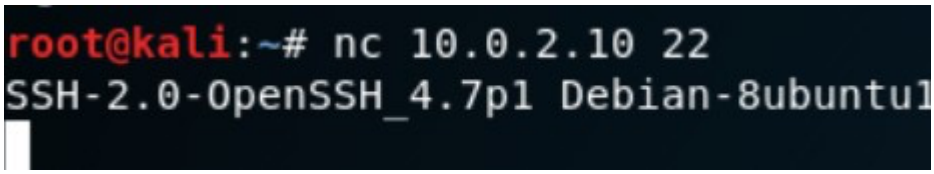


Рисунок 5 Захоплення банера за допомогою “ netcat ”

2.5 Високопродуктивні кібератаки

Тільки хакер виявить уразливість, яку він вважає придатною для експлуатації, він може розпочати Атакувати телекомунікаційну ціль, зосередившись на цій конкретній ваді. Серед вразливих установок ми можемо згадати веб-програми, веб-сайти, внутрішні мережі або Wi-Fi мережі. Представити їх всі просто неможливо, оскільки їх занадто багато, а нові все ще відкриваються, обговоримо лише основні. Вони найпоширеніші, оскільки шкода, яку можна заподіяти, є відносно важливо, а технічні норми повинні бути мінімальними.

Порушена автентифікація та управління сеансами

Аутентифікація - це процес, який полягає у підтвердженні своєї особистості, службі чи веб-сайту щоб мати доступ до ресурсів, щоб уникнути повторення цього процесу для кожного запиту, дані сеансу генеруються і ресурси будуть доступні, поки користувач не вирішить ввійти в систему чи вийти назовню.

Уразливість Веб-серверів та Веб-додатків.

Користувач повинен буде увійти використовуючи комбінацію імені користувача та пароля. Якщо ця операція неправильна, зловмисник може взяти обліковий запис, таким чином, діючи як дійсний користувач, або навіть

гірше як адміністратор. Якщо генеруються дані сеансу, такі як файли cookie, їх також можна вкрасти. (The OWASP Top 10: Broken Authentication & Session Management, 2018)

Пряма атака.

Щоб використати це, зловмисник має два варіанти. Першим було б спробувати атаку *Грубою силою (перший варіант),* тобто шляхом тестування загальної комбінації пароля користувача. Це можна зробити за допомогою атаки на основі словника, використовуючи файл, що містить список слів, сприйнятливих для використання, як паролі, як-от "пароль" або "123456789", або за допомогою рандомізованої комбінації тобто звичайні символи, спеціальні та цифри.

Другий варіант - спробувати захопити ідентифікатор сеансу, сформований, коли користувач успішно ввійшов в систему. Якщо ці дані не захищені, достатньо використовувати снифер для захоплення трафіку
щоб хакер прикидався зареєстрованим користувачем.

2.6 Атаки зовнішніх сутностей XML

Деякі веб-служби приймають XML-документи та обробляють їх. Відповідальна програма для обробки документів називається синтаксичний аналізатор XML і не обходиться без своїх ризиків. Якщо його неправильно налаштували, аналізатор XML може приймати зовнішні сутності, які є посиланнями. Зловмисник може зробити так, щоб ці зовнішні сутності посилалися на файли, з яких отримувалася система, яка обробляє файл XML. У більшості випадків метою є доступ до конфіденційних файлів, але також може призвести до атаки відмови в обслуговуванні.

Пряма атака

За допомогою текстового редактора підробити зловмисний файл XML легко. Це просто потрібно зрозуміти як працює аналізатор XML і як він може повернути нам конфіденційну інформацію.

Наведемо приклад , документ XML просить сервер Unix надати вміст “passwd” файл.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
  <!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
  <foo>&xxe;</foo>
```

Рисунок 6

Приклад атаки XML Exernal Entity (Top 10-2017 A4-XML External Entities (XXE), 2018)

Сервер буде шукати запитуваний ресурс і повертати користувачеві вміст файлу, розкриття інформації про рахунки. Важливо знати, що файли в мережі сервера також доступний.

2.7 Атака HTML-коду

Немає сумнівів, що більшість веб-сайтів містять документи HTML. Розкриємо, як зловмисні хакери знаходять конфіденційну інформацію з HTML-коду та як вони можуть використовувати команди SSI для управління веб-сервером. Крім того, розгляднемо недоліки вбудовування невідомих аплетів у веб-сайт.

Візьмемо, наприклад, браузер Firefox. Користувачі можуть знайти HTML-код, натиснувши Перегляд і вибравши Джерело, або одночасно натиснувши Ctrl та u. Наступний приклад ілюструє, як зловмисник перевіряє конфіденційну інформацію з HTML-кодів.

```
<!— Note to developers, please use the following directory structure /inet/html /inet/cgi-bin /inet/dev —>
<HTML>
<HEAD>
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=windows -1252"> <META NAME="GENERATOR" CONTENT="Microsoft FrontPage 4.0">
<META NAME="ProgId" CONTENT="FrontPage.Editor.Document"> <TITLE>Welcome</TITLE>
</HEAD>
<BODY>
<P>Welcome to our Web site</P>
<P><IMG BORDER="0" SRC=" file:///C:/inet/brick.jpg"></P>
</BODY>
</HTML>
<! — Further information can be acquired from the Administrator at (555)555-5555, ext. 1234 or via email at mcross@microsolved.com—>
```

Рисунок 7 Приклад цільового HTML-коду для зловмисника

Виділені частини показують конфіденційну інформацію у джерелі HTML. Перший рядок виділення - це примітка адміністратора, що пояснює структуру каталогів. Документи HTML зберігаються в каталозі / inet / html, сценарій CGI (Common Gateway Interface) знаходиться в / inet / cgi-bin, а веб-сайт зберігається в / inet / dev. Друга основна частина також відображає структуру каталогу. В кінцевому підсумку примітки адміністратора, які містять контактну інформацію адміністратора. У цьому прикладі він нагадує веб-адміністраторам переглянути всі опубліковані веб-сторінки HTML-кодів та видалити або змінити конфіденційну інформацію, якщо вона буде знайдена. Крім того, адміністратори також повинні налаштувати належні дозволи для каталогу на своєму сайті, тому відвідувачі не можуть отримати доступ до каталогу.

2.7.1 Включення сторони сервера SSI

SSI - це команда управління веб-сервером, яка може бути вбудована в HTML-коди. Це ще одна проблема безпеки, яку потрібно вирішити. По-перше, давайте візьмемо кілька прикладів, щоб побачити, як зловмисники використовують SSI.

```
Example 1
The current time is <!-#echo var="DATE_LOCAL"->

Example 2
<!-#include file="email.htm"->

Example 3
<!-#exec cgi=" /cgi-bin/test.pl"->
```

Рисунок 8 Приклад цільового HTML-код для зловмисника

Знак (#) вказує веб-серверу, що наступним кодом є команда SSI. У прикладі 1 "echo" - це команда, яка вимагає, щоб веб-сервер друкував певні дані в клієнтському браузері. Код "var =" змушує сервер знаходити змінну, яка називається DATE_LOCAL, тому веб-сервер буде друкувати поточний місцевий час у браузері клієнта. Змінюючи змінну, зловмисники можуть використовувати команду echo для друку необхідної інформації. Наприклад, зловмисники можуть змінити змінну прикладу 1 на DOCUMENT_URI, що є іншою поширеною змінною в SSI, і DOCUMENT_URI відображає зловмисникам поточні імена документів та шлях. У другому прикладі команда "включати" повідомляє веб-серверу викликати інший файл до HTML-документів, щоб у цьому випадку покупці побачили текст або зображення з файлу "email.htm". Якщо адміністратор не встановив належний дозвіл для конфіденційних документів, зловмисник використовує команду "включити", щоб знайти вміст цих документів, який може включати номер кредитної картки покупців або іншу інформацію. Команда "exec" виконує програму в системі або запускає файл сценаріїв оболонки. Зловмисники можуть керувати веб-сервером, використовуючи цю команду з іншою технікою. Якщо веб-сайту не потрібна ця команда, його адміністратор може відключити її, вибравши опцію "IncludesNOEXEC". Ці приклади є найпоширенішими методами атаки з використанням рекомендацій SSI, тому адміністратор повинен бути в курсі правильного встановлення дозволів, якщо веб-сайт застосовує функцію SSI. Більшість веб-серверів автоматично вмикають функцію SSI, тому веб-сайти повинні включати\ вимкати цю

функцію, коли вона їм не потрібна. Мережеві адміністратори можуть використовувати брандмауер для блокування SSI, якщо його неможливо вимкнути з веб-сервера.

2.7.2 Java, JavaScript та ActiveX

Java - це мова програмування, розроблена Sun Microsystems, і її часто використовують для виготовлення аплетів. Ці аплети можна вбудувати в коди HTLM, і вони працюватимуть у системі покупців, коли покупці завантажать коди HTLM в пам’ять своїх комп’ютерів. Ці аплети можуть стати цілями зловмисників. Зловмисники можуть спотворити програму Java і встановити в програму комп'ютерного хробака. Коли покупці відвідують веб-сайт, вони завантажують документи HTLM, які містять віруси в пам’ять своїх комп’ютерів, і ці хробаки зберігаються в системі покупця. Результат цієї атаки впливає на комп'ютери покупців, але це не впливає на веб-сервер. Але покупці зрозуміють, з якого веб-сайту походить цей вірус, після пошкодження їх системи. Наслідком цього буде зниження кредитної репутації веб-сайту. ActiveX працює майже так само, як аплети Java; він вбудований в документи HTML і запускає аплети після того, як покупці завантажать їх у пам'ять своїх комп'ютерів. Різниця між Java та ActiveX полягає в тому, що Java можна запускати практично в будь-якій операційній системі, включаючи Windows, Linux та Macintosh, тоді як компоненти ActiveX розподіляються як скомпільовані двійкові файли, тому вони працюватимуть лише в операційній системі, для якої вони були запрограмовані. В основному ActiveX спочатку працює лише з Internet Explorer. Через цю проблему безпеки Microsoft опублікувала компонент під назвою Authenticode для перевірки елементів керування ActiveX. Коли веб-сторінка намагається встановити елемент керування ActiveX, Authenticode перевіряє видавця цифрового підпису, щоб переконатися, що зловмисники не

змінили оригінальний код. Як щодо JavaScript? JavaScript - це мова програмування, яка може виконуватися в браузері клієнта, і вона дозволяє миттєво перевірити дані форми. Ця функція JavaScript зручна для покупців. Але JavaScript може містити і шкідливі коди, особливо коди, написані невідомими сторонами. Чи можна зменшити такий вид аптечних шахраїв? Відповідь позитивна. Перш за все, програмістам потрібно прочитати код кожного аплету, перш ніж застосовувати його в HTML-коді.

Програмісти повинні розуміти цілі коди аплетів і гарантувати, що коду можна довіряти. В іншому випадку вони не повинні використовувати ці аплети необдумано. По-друге, продавці можуть вибирати аплети та компоненти ActiveX, які створюються відомими компаніями. Наприклад, Microsoft пропонує на своєму веб-сайті багато зразків коду, які адміністратори можуть використовувати на веб-сайті електронної комерції. Покупці повинні прочитати ті інформаційні поля, які спонукають користувачів встановити елемент керування ActiveX. Покупці можуть вимкнути функції Java, JavaScript та ActiveX у своїх браузерах. На рисунку 9 показаний приклад вимкнення Java та JavaScript у браузері Firefox.

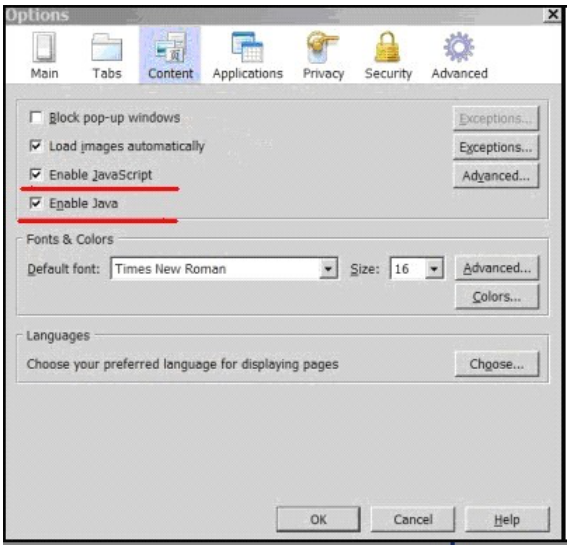


Рисунок 9 Параметри Firefox для ввімкнення / вимкнення JavaScript та Java.

Порушений контроль доступу

Коли користувач успішно входить в систему, права авторизації застосовуються відповідно до його привілегій.

Уразливість

Ризик тут з’являється після аутентифікації на веб-сайті або веб-програмі. Якщо не обробляти належним чином, користувачі без дозволу можуть отримати доступ до конфіденційних документів або навіть видалити або

змінити дані.

Пряма Атака

Для використання цієї вразливості потрібен лише браузер та певні знання про веб-сайт, які вимагаються. Оскільки доступ був погано налаштований, простий користувач, яким не повинен бути здатний виконувати деякі дії, може отримати доступ до ресурсів, просто змінивши URL-адреси. Це означає: Наприклад, зловмисник може вимагати перегляду сторінки адміністратора. У серверній частині жодної перевірки нічого не

зроблено, а особу та роль користувача не підтверджено, тому сторінка відображатиметься.

Якщо API додає, змінює або видаляє елемент за допомогою URL-адреси з певним синтаксисом, користувач може це зробити. (Порушений контроль доступу)

Рисунок 10 Виклик API для видалення елемента

2.8 Помилкові налаштування безпеки

При впровадженні нової служби або розробці нової програми, конфігурація за стоїть замовчуванням. Потім розробники або спеціалісти повинні пройти налаштування та змінити такі, які можуть створити потенційну ваду та усунути все, що виключно використовується для цілей уразливості.

Уразливості

Зловмисники можуть дуже легко виявити помилкові конфігурації системи безпеки завдяки чому можуть виконувати різні дії, якщо вразливості успішно використані. Ці помилкові конфігурації стосуються багатьох аспектів веб-додатків, але найбільш небезпечним є збереження конфігурації за замовчуванням для будь-якого елемента інфраструктури чи телекомунікаційної системи.

Системи управління вмістом (CMS) за замовчуванням дозволяють кожному встановлювати розширення, які є практичним при розробці, але його слід якомога швидше обмежити (Sucuri Blog, 2018). Якщо веб-сервери не налаштовані, це може бути проблемою, оскільки паролі за замовчуванням такі слабкі і легко вгадуються для нападника. Перерахування каталогів також

дозволено за замовчуванням, а помилки дають занадто багато інформації для можливого зловмисника.

Атака

Часто для здійснення атаки достатньо браузера. Залежно від CMS, шукають
"Admin.php" або "hidden.php" може бути успішним. Спроба дуже поширених паролів або, якщо потрібно, використання атаки грубої сили на основі словника також може призвести до успішного захоплення
над обліковими даними, і таким чином отримувати доступ до конфіденційної інформації.

Міжсайтові сценарії

Цю вразливість можна знайти на форумах або будь-якому веб-сайті, що дозволяє користувачеві розміщувати повідомлення, які відображатимуться на сторінці. Веб-сайти, які мають функціонал пошуку, є також хороший приклад.

Уразливість

Між сайтовий сценарій (XSS) полягає у введенні коду Javascript у веб-сайт.

Мета - змусити браузери інших користувачів запускати шкідливий сценарій. Уразливість приходить від небезпечних API Javascript і може мати великі наслідки для користувача-жертви, оскільки він вважає веб-сайт безпечним. Можна перенаправити користувача на різні сторінки, вкрасти навігаційні файли cookie, облікові дані тощо (Міжсайтові сценарії (XSS), 2018)

Атака

Ця атака може бути різною. Простим прикладом може бути коментар, залишений на веб-сайті, подібному до "<script> попередження (" XSS-атака успішна ") </script>" Тепер кожен раз, коли користувач відкриває сторінку з браузером, вважаючи, що це дійсний сценарій, вони це і роблять привітальним застереженням. У цьому випадку це не згубно, але, маючи трохи фантазії, зловмисник може надіслати користувачеві cookie-файл, приховуючи його за тегом "<img>", як показано нижче.

```
<script type="text/javascript">
  var addr = "http://www.serveur-distant.net/page-
piege.php?cookie=" + document.cookie;
  var imgTag = document.createElement("img");
  imgTag.setAttribute("src",addr);
  document.body.appendChild(imgTag);
</script>
```

Рисунок 11 Код Javascript, який надсилає файли cookie користувача на сервер зловмисника

Інший варіант - перенаправити користувача на підроблену веб-сторінку, яка запитає його ім’я користувача і пароль, а потім викрасти облікові дані.

Небезпечна десеріалізація

Серіалізація - це термін програмування, що означає перетворення об’єкта на потік байтів. Це робиться для того, щоб його можна було зберегти на диску або надіслати через мережу. Цей процес є можливий багатьма мовами програмування, і багато фреймворків це дозволяють. Десеріалізація є зворотний процес, перетворюючи потік байтів в об’єкт.

Уразливість

Десеріалізація може мати вразливі місця. Зловмисник може надсилати дані, що призводять до віддаленого доступу виконання коду або відмова в обслуговуванні.

Пряма атака

Реалізація цієї атаки може бути складною і характерною для мови програмування використовується для серіалізації об’єктів. Загальними недоліками є те, що сервер приймає ненадійні дані і використовує слабкі методи десериалізації.

2.9 Введення SQL

Введення SQL дуже популярне, оскільки його легко виконати. Якщо веб-додаток або веб-сайт дозволяє користувачеві запитувати базу даних для отримання інформації, вона може бути вразливою до цього маніпуляція.

Уразливість

Інжекція SQL - це техніка злому, яка полягає у зловмисній модифікації виконаних запитів до бази даних. Це часто робиться через веб-додаток і може мати руйнівний ефект щодо бізнесу компанії, оскільки елементи можуть бути отримані, або дані можуть бути змінені або видалені. Це можливо в основному через погане програмування.

Пряма атака

Для атаки не потрібні інструменти, лише знання про SQL. Давайте уявимо просту сторінку входу з користувачем та паролем. Якщо ми введемо "user1" для першого запису та "hello" для другого, базовий запит SQL, який перевірить, чи користувач використовує правильний пароль
“ОБЕРІТЬ * ВІД користувачів, ДЕ користувач =‘ користувач1 ’та пароль =‘ привіт ’”.
Якщо жодної перевірки не зроблено, будь-хто міг ввести таку пару значень: "user1", "OR 1 = 1--".
Це означає, що наступний запит буде виконаний базою даних:
“ОБЕРІТЬ * ВІД користувачів, ДЕ користувач =‘ користувач1 ’І пароль =’ ’АБО 1 = 1--’ ”, що завжди буде правдою. Це один простий приклад функціонування інжекції SQL, але атаки можуть бути результатом інших стратегій, таких як додавання оператора UNION для приєднання

Оператор SELECT, який поверне інформацію, яка не повинна розголошуватися.

2.10 Соціальна інженерія

Атака соціальної інженерії відрізняється від інших видів кібератак, оскільки не відрізняється, завжди не можливо передбачати злом. Він полягає в тому, щоб натомість зосередитись на людських слабостях та технологічних недоліків.

Уразливість

Люди є найбільш вразливою частиною телекомунікаційної системи. Ними можна маніпулювати, щоб розкрити їхню конфіденційну інформацію або несвідомо дозволити хакеру отримати доступ до ресурсів. Тактика, що використовується, часто використовує брак знань та обережність жертв.

Пряма атака

Виконання атаки соціальної інженерії вимагає від зловмисника деяких якостей, таких як самовпевненість та винахідливість. Методи різноманітні, але більшість випадків злочинець спробує переконати працівника компанії дати конфіденційну інформацію шляхом удавання бути кимось іншим, або телефоном, електронною поштою, або навіть особисто. Бути таким же переконливим і як можна тонше, він намагатиметься отримати необхідну інформацію без її справжньої ідентичності бути викритим. Зловмисник також може побічно обдурити співробітників, щоб вони здійснили маніпуляцію, яка скомпрометує компанію. Цей прийом під назвою фішинг складається з надсилання електронного листа з підробленим вкладенням або зловмисне посилання. Часто прикидається другом, колегою по справі партнера чи великої організації, вміст має на меті спонукати користувача відкрити вкладення або натисніть на посилання. Відкриття вкладення може призвести до шкідливого програмного забезпечення, яке може відкрити порти на комп’ютері жертви або видалити файли. Існує безліч дій хакера, яке може виконуватись таким чином. Посилання можуть перенаправляти користувачів

на підроблені веб-сайти, що підбурюють жертву введіть його дані (на приклад: підроблена сторінка входу в Gmail, це є підроблена сторінка входу з банку і т.д.).

Ключ до успішної атаки соціальної інженерії - зробити так, щоб жертва нічого не підозрювала, використовуючи подібні посилання, як відомі, популярні рецепти тощо. Якщо хакер рішуче налаштований напасти на бізнес, він також схильний до злому ділових партнерів раніше, і використовуйте їх електронну пошту, щоб змусити жертву думати, що посилання або вкладення надходить від довіреного джерела.

3 МЕТОДИ ПОБУДОВИ КІБЕРЗАХИСТУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

3.1 Методи запобігань кібератак

Існуючі методи запобігань, які необхідно застосовувати для кожної з представлених атак. Крім того, найкраща стратегія виправлення цих уразливостей - це наявність декількох способів нейтралізації атаки. Послідовності дій, такі як керування введенням користувача перед його обробкою та виконанням операції пізніше в логіці додатків - хороша практика, що розвивається. Застосування захисту на кілька шарів системи означає, що хакер повинен знаходити недоліки в декількох компонентах. (Solarwinds MSP). Крім того, використання бібліотек може допомогти у розробці безпечних програм. Доступний практично в будь-якій мові, конкретні інструменти або рамки застосовують і застосовують механізми безпеки, щоб уникнути найпоширеніших нападів.

Не надійна аутентифікація та управління сеансами

Оскільки зловживання паролем грубої сили є основною загрозою тут, може бути порушена аутентифікація, ця проблематика вирішена шляхом недопущення декількох спроб входу за короткий проміжок часу. Система повинна також запобігати введенню помилкового пароля більше, ніж визначену кількість разів. Крім того, співробітники повинні використовувати надійні та непередбачувані паролі. Ідентифікатори сеансів повинні бути захищені. Він не повинен відображатися ніде, як в URL-адресі, і бути захищений богаторівневим шифруванням.

3.2 Атаки зовнішніх сутностей XML

Якщо телекомунікаційна система використовує синтаксичний аналізатор XML, його слід налаштувати та вибрати конфігурації які налаштовані за замовчуванням, тобто необхідно їх змінити, оскільки зовнішні сутності

можуть не бути відключені (Top 10-2017 A4-XML Зовнішні організації (XXE), 2018).

Більше того, якщо сервер не має прав на доступ до важливих файлів, він може видавати їх вміст зловмиснику. Потрібно застосовувати принцип найменших привілеігій: він марний, тобто небезпечно надавати серверу максимальні привілегії, якщо він у цьому не потребує. Найкраща практика надати ті самі права, що й найменшому абоненту.

3.3 Оновлений контроль доступу

Часто виникає внаслідок виникнення помилок або упущень, непрацездатних вразливостей контролю доступу, які можна легко перевірити. Якщо дію виконує користувач, який не повинен мати прав для цього. Знання місця перевірки є надзвичайно важливим, тому маючи хороший контроль, політика доступу може допомогти уникнути цих неприємних ситуацій. Деякі найкращі практики також включають ні виставляти ідентифікатори користувачів або іншу корисну інформацію для хакера в URL-адресі та не залишати приховані сторінки на веб-сайті.

3.4 Стандартні налаштування систем безпеки

Витратити час на налаштування служб і знати, як вони функціонують - найкращий спосіб уникнути від атак та ситуацій від яких страждає телекомунікаційна система, тобто від неправильно налаштованої конфігурації. Стандартні налаштування за замовчуванням слід залишати лише тоді, коли впевнені, що безпека гарантована.

3.5 Міжсайтовий сценарій

Міжсайтовий сценарій може статися, коли зловмисник заповнює текстове поле зловмисним кодом. Щоб уникнути це, можна перевірити його вміст і заборонити користувачеві використовувати певні символи, як-от "<" та ">" у цьому випадку. Інше рішення, якщо дозволено бути всім символам

використовується для кодування даних, введених користувачем, у HTML. Таким чином, вміст не буде інтерпретуватися браузером як Javascript. Оскільки атаки XSS також можуть відбуватися, коли зловмисник змінює URL-адресу, це важливо щоб переконатися, що URL-адреси також закодовані. Важливо застосовувати методи в БЕКЕНД, щоб переконатися, що URL-адреси та текстові поля безпечні (Microsoft, 2018).

3.6 Десериалізація

В першу чергу небезпека виникає коли вводяться дані, які потенційно не є безпечними. Перший метод - зосередитись на даних, які будуть серіалізовані, перевіряючи те, що введено, та обробляючи їх правильно. Оскільки атака характерна для використовуваної мови програмування, використовуючи хороші бібліотеки та безпечний метод у бекенді важливо. (Мессіна, 2018)

3.7 Введення SQL

Основною рисою усіх методів та методок є якомога менше розкривати інформацію зловмиснику щодо телекомунікаційних систем. Якщо видається помилка бази даних, хакер краще зрозуміє, як запити обробляються, і ми будемо робити щось інше.

Ризик SQL Injection надходить із текстових полів, першим і найбільш очевидним рішенням є перевірка введених значень та заважання користувачам вводити певні символи, наприклад одинарні цитати або дефіси. Використання параметризованих запитів, які також називають підготовленими операторами, є найкращий спосіб усунути ризики введення SQL.

Якщо хакер вважає, що веб-програма вразлива для цього типу атак, він, швидше за все, це зробить, необхідно спробувати виконати різні дії над

базою даних, щоб знати її схему. Все зберігається в log файлах, тому різні шаблони цього файлу можуть виявити спробу введення SQL.

3.8 Соціальна інженерія

Щоб уникнути атак соціальної інженерії, люди, які працюють у компанії де розвинена телекомунікаційна мережа, повинні бути підозрілими постійно, коли дзвінок або електронне повідомлення надходить з невідомого джерела.

Найкращий спосіб запобігання цьому виду нападів полягає в інформуванні працівників та допомозі їм розпізнати характеристики або загальні шаблони. Наприклад, злочинець, який намагається маніпулювати жертвою, буде часто
робити вигляд, що ситуація надзвичайна або надзвичайно важлива, щоб мінімізувати час людині думати і використовувати стрес як перевагу. Коли співробітники повинні бути недовірливими не дотримуються стандартних процедур, і виникають запитання щодо конфіденційних даних чи запитав. Для фішинг-атак, хоча антивіруси не є на 100% безпечними, вони ефективно виявляють зловмисні вкладення та блокування вхідної електронної пошти або попередження працівника. Посилання є
складніше мати справу з ними, оскільки вони можуть легше обійти безпеку. Співробітники повинні визначати та розпізнавати в першу чергу ризикв фішингу, а також, як розрізняти фальшиві URL-адреси, веб-сайти та ієрархію різноманітних прикладів зловмисних електронних листів.

4 ЗАГАЛЬНІ ТЕХНІЧНІ РЕКОМЕНДАЦІЇ

4.1 Загальні рекомендації

На сам перед розглянемо дві основні причини, чому телекомунікаційні системи не докладають достатніх зусиль захищеності.

Перша причина - відсутність знань і не уявлення того, що може статися з їх мережою. Це стосується невеликих телекомунікаційних мереж, які мають обмежену кількість техніки, і ніхто не знає, наскільки небезпечно мати вразливі місця. Можливо, вони знають, що їх телекомунікаційна система може бути скомпрометована, але оскільки вони ще не зазнали жодної атаки, адміністратори таких систем вважають, що вони є захищеними, хоча порушення може статися в будь-який час, якщо цього ще не сталося. В деяких випадках хакери мали доступ до ресурсів та конфіденційних документів, але з тих пір ніхто в IT-відділі не помітив порушення, і нічого руйнівного не було зроблено, усі в телекомунікаційній мережі не могли подумати, що це нормально, коли насправді хакери мали віддалений доступ на проміжоку тривалого часу.

Друга причина, через яку не застосовуються заходи безпеки, - це бюджет. Часто безпека викликає занепокоєння, але, на жаль, бюджет не дозволяє телекомунікаційним системам діяти відповідно до певних умов кібербезпеки. Знову ж таки, це особливо актуально для малого бізнесу, який просто не може дозволити собі великі заходи. Вони змушені або змінити свою діяльність, щоб дозволити невелику частину бюджету інвестувати в безпеку або реагувати на чуйну поведінку виключно тоді, коли вони відновлюють лише ті файли, які вони втратили, та виправляють уразливість, яка дозволила зловмиснику мати доступ до файлів. Історія обов’язково повториться, як це могли робити інші хакери використовувати всі виявлені вразливості, а іноді і те саме, якщо IT-команда не в змозі визначити точку

входу зловмисника. Це рішення не є ідеальним, і його можна зробити, лише якщо не зберігати конфіденційні дані про користувачів.
Незалежно від фінансових ресурсів, малому та середньому бізнесу слід брати на себе кібербезпеку серйозно. Навіть якщо досягнення непорушної системи неможливе, засоби повинні бути розгорнуті, щоб принаймні зробити телекомунікаційну систему чи мережу складною мішенню для злому. *Виконання розвідки* метод, складний для хакерів, і уникнення легкої експлуатації вразливостей повинно бути достатньо заохоченим зловмисником. Будь-яка невмотивована особа, яка має виключно намір напад піде в інше місце і, швидше за все, піде шляхом меншого опору. Заперечуючи доступ до людей з поганими хакерськими знаннями та сценаріями, які просто шукають простої здобичі - це метод у правильному напрямку. Легкі цілі для хакерів можуть бути малими і середніми мережами, основний бізнес яких не має нічого спільного з IT, і нещодавно прийняли нові технологій. Будівництво або промисловість в основному схильні до нападу.

4.2 Рішення та стратегії з кіберзахисту

Знання того, які інструменти та стратегії застосовує зловмисник, означає, що телекомунікаційна система може захищати себе, повторюючи різні кроки, виконані для компрометації їх встановлення. Якщо захист даних або послуг, залежно від серверів, видається пріоритетом, це необхідна допомога IT-спеціалістів або білих хакерів. Цифра також називається етичною,
хакер особливо цікавий тим, що він володіє знаннями і волею до співпраці з телекомунікаційною системою для захисту від своїх зловмисників.

Кібербезпека - це питання ризиків. Угода полягає в тому, щоб знати, на який ризик готова піти телекомунікаційна система та її власники з точки

зору кібербезпеки, які елементи є найбільш критичними та куди вкладати гроші.

Дуже важливо поговорити про ризики та мати точні знання про те, що може статися, оскільки іноді компанії можуть неохоче витрачати гроші, щоб захистити свої активи. Оскільки вони не можуть безпосередньо зрозуміти, наскільки це їм вигідно (на відміну від нового принтера або нових комп'ютерів), вони вагаються, щоб захистити себе правильно, і вважають це марною тратою грошей.

Першим кроком до створення плану безпеки є оцінка ризику. Не кожен бізнес однаковий. Процеси, що стосуються безпеки, повинні бути повністю адаптовані до діяльності працівників, взаємодія із замовниками та технічна інфраструктура. Захист також передбачає хороші бізнес-процеси, що враховують аспекти безпеки. Визначення засобів захисту на підприємстві практично нічого не коштує, тому ні лише малий бізнес, але середній та великий, можуть і повинні визначати та застосовувати деякі рекомендації щодо отримання найкращих результатів.

4.2.1 Стратегії та найкращі методи

Є кілька методів, які виявилися успішними та надійними проти різних форм кібератаки. Такі технічні рішення, як наведене нижче, можуть стати гарним покращенням для кібер безпеки всередині телекомунікаційної мережі.

Скорочення доступної інформації. Першим кроком атаки, проведеної досвідченим кіберзлочинцем, є, як уже було видно, це footprint. Деякі елементи неможливо видалити, але будь-яку інформацію, що стосується операційної системи сервера, технології або використовувана версія повинна бути прихована від ззовні. Якщо ці примітки відображаються у файлах HTML, їх потрібно виключити. Те саме стосується сервера Apache екран

помилок, що відображає його версію, і так далі. Головна ідея - мати постіне спілкування з розробниками, щоб мінімізувати ці ранні ризики.

Безпечний розвиток для телекомунікаційної мережі

Намір зробити безпечну послугу або програмне забезпечення має існувати з самого початку, і ще більше, розробка безпечного продукту має бути одним із пріоритетів. Інженери-програмісти в ідеалі повині мати уявлення про найкращі практики, інакше експерт з кібербезпеки повинен допомогати їм та створити кінцевий результат без уразливих місць, якщо це можливо. Це також має перевагу в скороченні робочого часу, аналіз роботи в подальшому, змушуючи розробників виправити можливі недоліки забирають більше часу, ніж застосування директив.

Політика паролів

Примусити працівників застосовувати надійні паролі дуже важливо для любої телекомунікаційної мережі. А більшість користувачів мають однаковий пароль для кожного облікового запису, який вони мають, і якщо він є один раз скомпрометований, це може поставити мережу під загрозу. В даному випадку необхідно примушувати їх мати новий, так виключається ризик того, що зловмисник просто введе пароль, з якого він уже знає. Наявність складних паролів також може виключити ризик атак грубої сили, оскільки потрібні роки, щоб зламати довгу і складну низку символів. NIST опублікував нові вказівки щодо паролів 25 квітня 2019 року та запропонував рішення, адаптовані до поточного часу (Рекомендації щодо цифрових ідентифікаційних даних, 2019).

Це не так обов'язково застосовувати всі з них, але впроваджуючи деякі найкращі вимоги, включаючи вставляючи спеціальні символи, мають мінімальну довжину та уникаючи передбачуваних паролів. Якщо використовується Active Directory, її можна налаштувати за допомогою групової політики.

Об'єкти (GPO).Сенсибілізація фішингу.

Найпоширенішими та успішно виконуваними атаками є фішинг-атаки, оскільки вони вимагають від зловмисника майже ніяких зусиль і можуть легко поставити під загрозу мережу, що робить його доступним віддалено. Цей метод існує вже давно, і хакери є все більш винахідливими, щоб переконати свою ціль. Не існує ідеальної частоти нагадування працівникам про цей тип загроз кібербезпеці, але це потрібно зробити. Вони не повинні забувати, що вони є найслабшим елементом з точки зору безпеки в мережі.

Видалення невикористаних профілів

Хорошою практикою для кібербезпеки є позбавлення від усього, що не потрібно, і не стосується служб, що працюють на сервері. Старі облікові записи користувачів все ще вразливі, і якщо зловмисник може підняти цей профіль, знайшовши його пароль, у нього є власний обліковий запис в мережі, не знаючи нікого, і не втрачаючи часу, щоб спробувати встановити свої привілеї.

Оновлення

Другою за величиною причиною, яка спричиняє порушення та витоки даних, є невиправлені помилки вразливості. Найвідоміший приклад - "WannaCry", який є вимога тором, використав вразливість першої версії протоколу SMB у 2017 році. Оскільки це Протокол, який використовують машини Windows для зв'язку, можуть усі комп'ютери в мережі заразитися та зашифрувати їх файли. Microsoft випустила виправлення, виправляючи це незабаром після цього, але деякі системи, які запізнились робити оновлення, були частиною 200’000 жертв програми-вимогача.

Zero-days vulnerabilities потенційно кожна послуга, якою користується система, може стати точкою входу для хакера, тому постійно оновлювати програмне забезпечення є найкращий спосіб захисту від такої форми нападу. Залежно від діяльності мережі, воно може бути складним, тобто необхідно тимчасово вимкнути служби для перезавантаження серверів, але в довгостроковій перспективі, це може заощадити багато грошей для компанії, навіть якщо це означає придбання вторинної машини виконати оновлення.

Резервне копіювання

У разі програми-вимагача чи будь-якої руйнівної атаки жодна мережа не може дозволити собі втратити всі свої дані без шансів отримати їх назад. Потрібно створити резервний план, а не лише запобігати випадкам кібератаки, а також технічним проблемам, які можуть виникнути. Важливо, що резервне місце також знаходиться в безпечному місці, за можливості поза мережею, щоб уникнути також скомпрометованих точок та документів.
Оскільки кібератака може статися в будь-який час, телекомунікаційним системам важливо визначити, як це зробити тобто відновити втрачені дані і як продовжити свою діяльність якомога швидше.

4.2.2 Аутсорсинг

Співпраця зі спеціалізованими компаніями, що займаються питаннями безпеки, можуть зробити великі вигоди, якщо за будь-яку ціну потрібно впровадити максимальну безпеку. Це стосується в основному великих телекомунікаційних систем, які можуть дозволити собі такі послуги. Ці спеціалізовані компанії мають перевагу у тому, що вони мають повну компетентність у своїх сферах. Хоча все одно потрібно, щоб люди всередині компанії дбали про кібербезпеку та дотримувались певних заходів, це дозволяє їм мати більше вільного часу, менше роботи та якісних порад у разі потреби. Заощаджується не лише час, але й гроші, оскільки часто пропоновані послуги є якіснішими та дешевшими, ніби їх робили власноруч. Деякі великі телекомунікаційні системи обробляють важливі дані, якщо їх установка не надто складна. Насправді аутсорсинг означав би обмін інформацією зі сторонніми компаніями і навіть якщо означає більші витрати, це найкраще рішення. Аутсорсинг може здатися найкращим рішенням для великих телекомунікаційних систем з малими телекомунікаційними мережами в різних місцях. Середні мережі також можуть скористатися цією стратегією, оскільки вона має досвід зовнішнього партнера при зменшенні вартості. Тільки мала мережа повина вибирати між дешевими та безкоштовними інструменти або відсутністю захисту взагалі.

Відповідність стандартам

Деякі IT-спеціалізовані компанії пропонують підготувати бізнес до відповідності стандарту і отримати сертифікацію. Найвідомішим стандартом з точки зору кібербезпеки є ISO 27001 від серії ISO 27000, які відносно безпеки. Він спрямований на створення ефективної система управління інформаційною безпекою, що складається з 4 етапів: планування, виконання,

перевірка та дія (ISO / IEC 27001: 2013, n.d.). Інший аспект - дотримання вимог GDPR, що набрало чинності наприкінці травня 2018 року.

Оцінка вразливості

Позитивним рисами для телекомунікаційних систем є те, що система усвідомлює, де її вразливі місця. Використання автоматизованого інструменту, які вони часто розробляють самі, експерти можуть з'ясувати сильні сторони та слабкі сторони або мережа, сервери, веб-сервіси тощо. Завдяки цьому вона створює міцну основу, як для малих, так і для більших телекомунікаційних систем.

Випробування на проникнення

Тестування на проникнення полягає у спробі обійти заходи безпеки системи, з різними інструментами для перевірки його ефективності. Якщо не визначена політика безпеки та критичні вразливості все ще присутні, тестування на проникнення не триватиме, і експерти доведуть, що є простий спосіб скомпрометувати систему. Ця вправа не має сенсу, якщо виконувати її передчасно і зарезервовано для систем, які вже мають надійні установки. Тестування на проникнення зазвичай проводить група експертів з компанії кібербезпеки, але є інший спосіб зробити це, що може призвести до дешевшого методу. Часто великі системи моделюють розгортання фальшивої служби і дозволяють будь-яким хакерам знайти вразливості місця та використовувати їх. Кожна успішно використана вразливість винагороджується. Ця система, що називається Бауті, має перевагу у тому, що має більшу кількість людей і намагаючись скомпрометувати свою систему до фактичного розгортання, протягом більш тривалого періоду. Якщо кількість вразливостей низька, цей метод тестування на проникнення буде таким дешевшим, ніж експерти, які оплачуються щогодини.

4.3 Технічні рішення

Кібербезпека значною мірою покладається на технологічні заходи. Впровадити оптимальний захист встановлення, необхідно мати знання та фінансові ресурси. Умова занадто часто визначає рівень безпеки організації, як це роблять деякі компанії неохоче інвестує в заходи безпеки, але є деякі речі, які можна зробити безкоштовно для підвищення рівня захисту. Ресурси компанії повинні бути в безпеці зовні, але також і зсередини. Працівники не повинні мати можливості виконувати певні завдання, як зміна інформації про клієнта або просто зробити щось руйнівне.

4.4 Стратегії з найкращіх методів кіберзахисту

Щоб успішно встановити кібербезпеку, слід дотримуватися деяких вказівок. це є важливим захистом від будь-якого шкідливого програмного забезпечення або зловмисних маніпуляцій, що надходять від зовні, а також зсередини.

Брандмауери та malware захист від шкідливого програмного забезпечення

Брандмауери та антивірус перш за все повинні бути встановлені на всіх машинах і бути сучасними. Це є мінімальним мінімумом з точки зору захисту та дозволяє працівникам працювати в безпечних умовах.

Управління послугами та інформацією один з простих способів хакера провести атаку - з’ясувати, який сервіс використовується і яка версія, щоб знайти відомі вразливості. Найкраще рішення для протидії цьому - це перш за все отримати-позбутися будь-яких невикористаних послуг. Якщо вони дійсно необхідні для діяльності системи.Оновленя серверів зробить роботу хакера-ще важчою, можна приховати версію служби або навіть змінити її в деяких випадках. Це змусить зловмисників втратити час і зменшить вплив

автоматизованих атак. Обмеження інформації також можна здійснити через DNS, забороняючи передачу зон DNS, якщо вони не надходять із надійного джерела.

Внутрішній захист

Якщо простий співробітник компанії може виконувати дії, обмежені адміністратором, це недолік. Якщо налаштовано Active Directory або будь-який тип бази даних для користувачів, це повинно запобігати тим, хто не має повноважень робити та небажаних операції, і потенційно компрометувати телекомунікаційну систему. Як це часто може бути випадковим, зловмисні дії проти компанії може зробити добровільно працівник.

Крім усього іншого, можна відкрити бекдори та вкрасти важливі дані, тому маючи контроль за тим, що підлеглі роблять у будь-який час, є великим плюсом для малих та середніх мереж, і стає все більш важливою, чим більшою вона стає.

Телекомунікаційна мережа

Відстеження того, що відбувається в мережі компаній, є прекрасним способом боротьби з атаками ззовні, а також всередині. Існує кілька найкращих практик щодо створення телекомунікаційних мереж, і серед найважливіших і найпростіших - це створення підмереж. Розділення групи комп'ютерів в окремих мережах можуть отримати перевагу, виділяючи потенціал пошкодження та уникаючи його поширення.

Шифрування

Конфіденційна інформація не повинна передаватися чи зберігатися як чистий текст. Це стосується паролів, номерів кредитних карток, а також особисті дані відповідно до GDPR.

Спілкування з користувачами, але також всередині системи, має бути забезпеченим. Третя сторона, яка не має ключа до розшифровки, не повина мати доступу до потоку даних. Це також можливо використовувати для

шифрування файлів для захисту конфіденційної інформації на серверах або конкретної комп’ютерої мережі.

4.5 Новітній рівень кіберзахисту

Якщо компанії в яких є своя телекомунікаційна система хочуть серйозно ставитися до кібербезпеки, існує безліч інструментів, які допоможуть їм вдосконалити їх безпеку. Це можливо досягти за рахунок профілактичних заходів. Деякі компанії з кібербезпеки пропонують ці переваги, але це можливо зробити самостійно, якщо IT-працівники мають достатньо знань та необхідних інструментів. Тобто в першу чергу йдеться про перевагу не ділитися будь-якими даними з потенційним діловим партнером, але і є мінус - не мати якісних інструментів, якими володіють ці спеціальні компанії. Це залежить від бюджету та людських ресурсів, а також законодавства, оскільки потрібні певні великі підприємства, такі як на приклад – банки, тобто йдеться про незалежну компанію, яка регулярно контролює їх встановлення.

Оцінка вразливості Сканування телекомунікаційної системи на наявність уразливостей дозволяє компанії легко побачити, де необхідно спрямувати зусилля. Виконуючи оцінку вразливості, досить зупинитися, коли з'явиться список вразливості. Експлуатувати їх поки що не потрібно. Доступно багато автоматизованих інструментів, найпопулярнішим та найреальнішим лідером маркера є Nessus. Доступний безкоштовно для особистого користування, але щомісяця Nessus дозволяє адміністраторам компаній виконувати різні типи сканування, наприклад виявлення шкідливого програмного забезпечення або сканування веб-додатків.

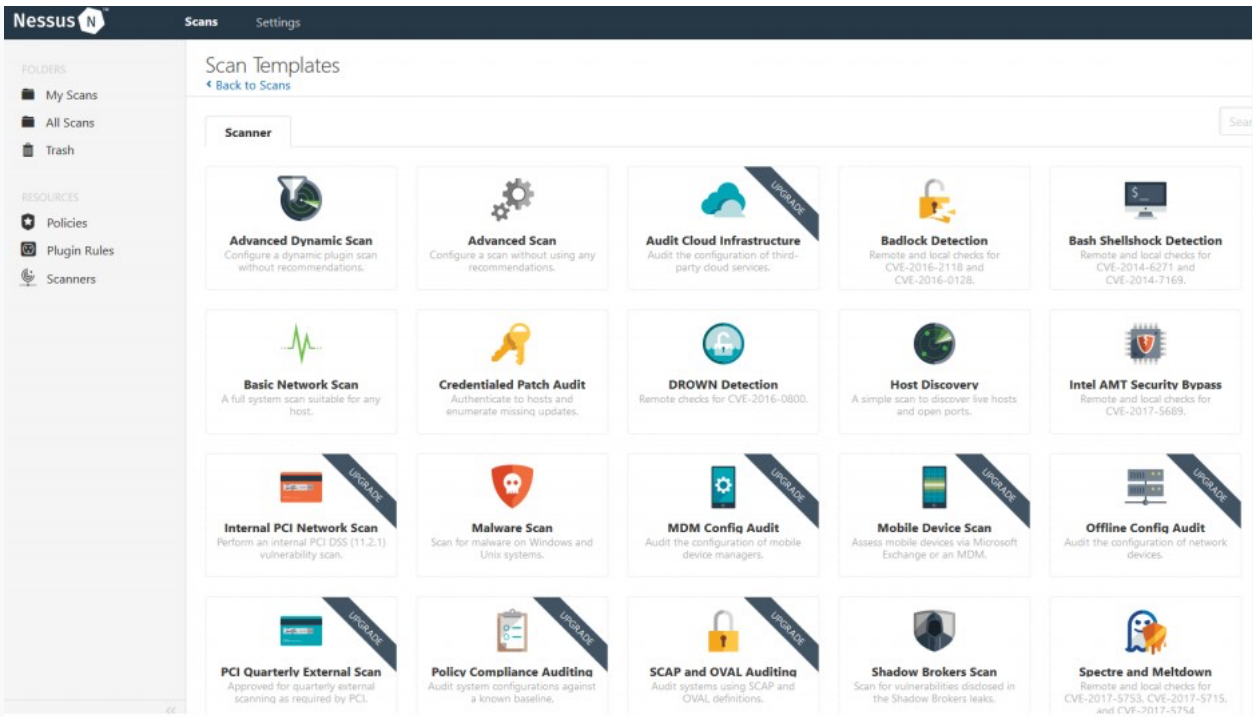


Рисунок 12 Сканування в Nessus

Nessus стверджує, що нові плагіни надходять щотижня, це означає, що Tenable залишається на вершині, а поле кібербезпеки вводить способи виявлення потенційних вразливостей на нульовий день.

Ця постійна зміна бази даних також означає виконання оцінки вразливості одного разу недостатньо. Рекомендується, залежно від результатів попереднього сканування та складність монтажу компанії, регулярно переходити до повної перевірки і переконуватись, що не з’явилася нова вразливість.

Програма “WannaCry” (яка шифрувала дані і відправляла їх на сервер якого не існує, а саме комедне, що після цього вимагала грощі за те що поверне шифровані данні) мала свій власний плагін у Nessus. Бізнес-процеси повинні визначати, коли відбувається кібератака, а співробітники служби безпеки повинні провести нову оцінку вразливості, оскільки це залежить від бізнесу малого, середнього чи малого.

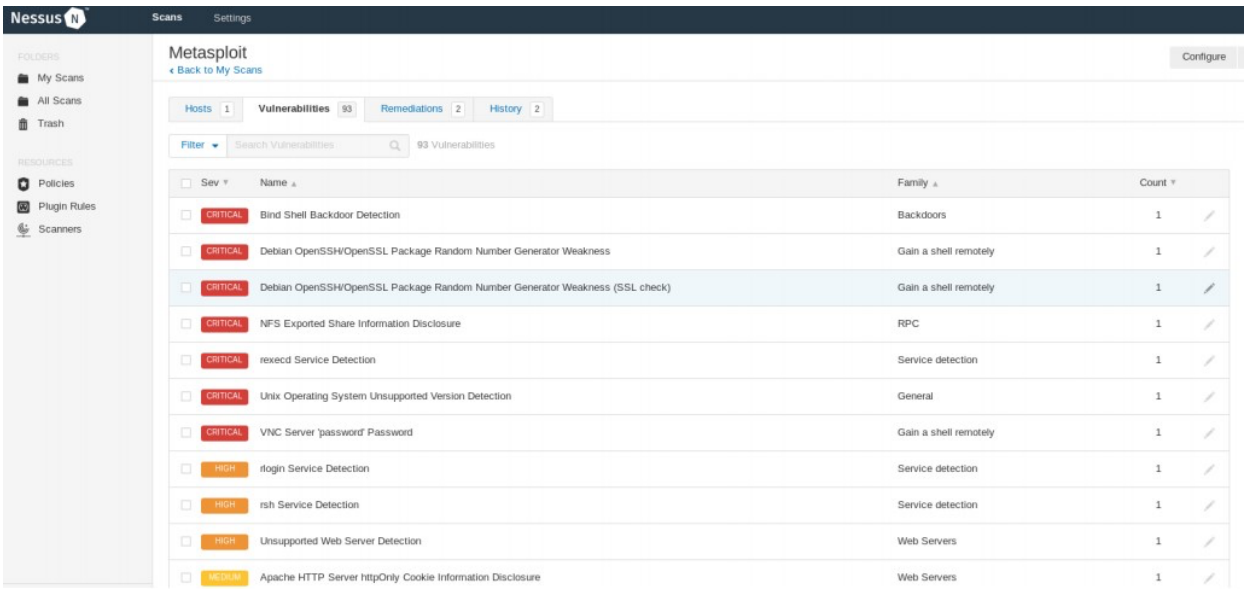


Рисунок 13 Оцінка вразливості з Nessus

Іншим популярним інструментом, що використовується для сканування вразливостей, пов’язаних з Інтернетом, є Burp Suite, і є доступна версії, але корпоративна - покриває велику кількість уразливостей включаючи ті, що входять до топ-10 OWASP, де перераховані найпоширеніші вразливості в веб-додатках. Можна періодично планувати сканування, щоб постійно перевіряти наявність нових вразливості.

Системи виявлення вторгнень

Системи виявлення вторгнень (IDS) мають на меті виявляти видимі закономірності підозрілими, і тим самим виявляючи наявність можливого шкідливого програмного забезпечення або зловмисника, який міг би вдало обійти брандмауер.

Існує 2 типи IDS.

Перший тип - це система виявлення вторгнень у телекомунікаційну мережу. Його роль полягає в аналізі мережевого трафіку і шукайте

потенційні загрози, а потім виконуйте дії відповідно до того, як це налаштовано (Мережева система виявлення вторгнень NIDS). Найпоширенішим інструментом є Snort, який являє собою програмне забезпечення з відкритим кодом.

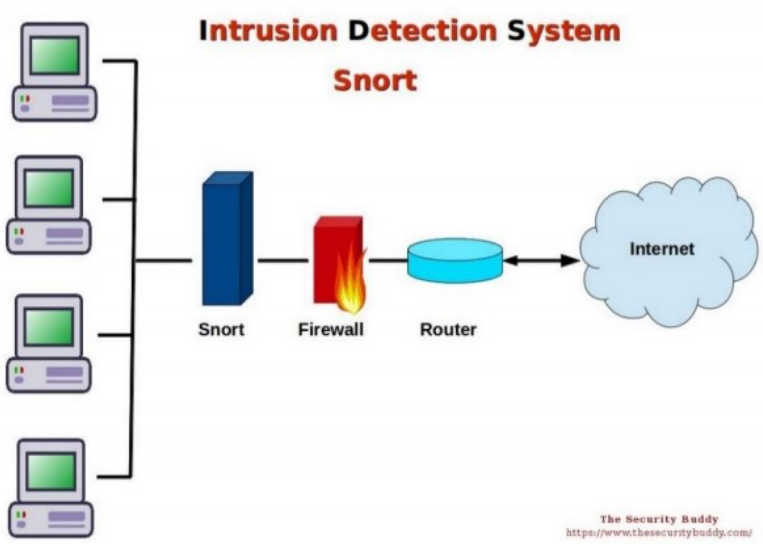


Рисунок 14 Snort в телекомунікаційній мережі

Snort можна налаштувати для виявлення деяких конкретних дій у мережі. Конфігурація файлу дозволяє вносити ці зміни, окрім стандартних. Також можна додати правила зроблені спільнотою, а також правила, створені командою розробників. Очевидно, що так необхідно бути в курсі цих правил, щоб отримати максимальну безпеку. (Налаштовуючи Snort IDS на Debian Linux).

Другий тип - IDS буде контролювати файли журналів із програм і сортувати їх, щоб збільшувати читабельність. Система виявлення вторгнень хоста (HIDS) повідомляє адміністратора про те, що підозрілий елемент виявляється в журналах, що може бути ознакою несанкціонованої особи, яка намагається маніпулювати файлами. IDS, який генерує попередження, коли виявляє певний шаблон, називається підписом, тоді як IDS, який генерує попередження через дивну поведінку користувача чи програми, наприклад

оскільки вхід з різних місць одночасно, називається аномалією (6 найкращих Інструментів систем виявлення вторгнень на базі хоста HIDS). Ці налаштування можуть бути налаштовані відповідно до діяльності певної компанії. Погано скориговані параметри призведуть до багатьох попереджень, які називаються помилковими спрацьовуваннями, або взагалі відсутні. Наявність низької чутливості означає, що IDS не вдалося виявити реальну загрозу, а занадто висока чутливість може призвести до збільшеного попередження, що потрібно буде проаналізувати працівнику, що може заняти дуже багато часу.

Випробування на проникнення

Тестування на проникнення або Pentest складається з перевірки безпеки компанії шляхом пошуку вразливості та їх використання. Люди, які намагаються скомпрометувати веб-додаток або телекомунікаційна мережа є білими хакерами і не буде завдаватишкоди. Чим більш досвідчені білі хакери, тим ефективнішим може бути захист.

Він називається "black box" пентестом, коли експерт, який виконує цю операцію, не отримує інформації про телекомунікаційну систему, яку він повинен атакувати. Він повинен думати і діяти як зловмисний хакер, знаходити вразливості та використовувати їх. На противагу цьому, зловмисник виконує «white box» pentest та отримавши IP-адреси та різні вказівки на систему. Два методи мають свої переваги та недоліки. Перший нагадує фактичну атаку, яка включає етап розвідки та більш ретельне сканування, тоді як другий дозволяє компанії провести більш поглиблений аналіз їх встановлення. Це також можна використовувати в обох стратегіях, які називаються "gray box".

Існують різні сфери, які можуть бути піддані pentest. Пошук порушень в мережі є найпоширенішим типом. У цьому тесті зловмисник намагається виконати декілька цільових атак на певні заходи, включаючи брандмауери та маршрутизатори. Він також побачить, як на проникнення реагує Система. Потім зловмисник може зосередитися на веб-додатках, веб-сайті, хмарі послуги або бездротову мережу, якщо у компанії є така. Є можливість перевірити внутрішню безпеку компанії шляхом внутрішнього pentest. У цьому випадку стандартний доступ отримує pentest і він намагатиметься виконувати дії, що вимагають вищих прав, або навіть виконувати привілегії ескалації. Ця перевага полягає в тому, що він усвідомлює, яку шкоду може нанести зловмисник, коли у нього є доступ до системи. Після випробування на проникнення складається звіт, висвітлення виявлених вразливостей, способу їх використання та наскільки вони небезпечні дані телекомунікаційні системі, а також рекомендації.

Основними перевагами pentest є знання того, які вразливості є і як зловмисники можуть скомпрометувати телекомунікаційну систему. Недоліки в телекомунікаційній системі суворо упорядковані, тому це хороший спосіб дізнатись, що слід визначити пріоритетними, і над чим можна попрацювати, також базуючись на рекомендаціях експертів.

Для проведення pentest на ринку 12 доступні різні інструменти, серед яких найпопулярніший Metasploit - це фреймворк, доступний для Linux та Windows, виготовлений Rapid7.

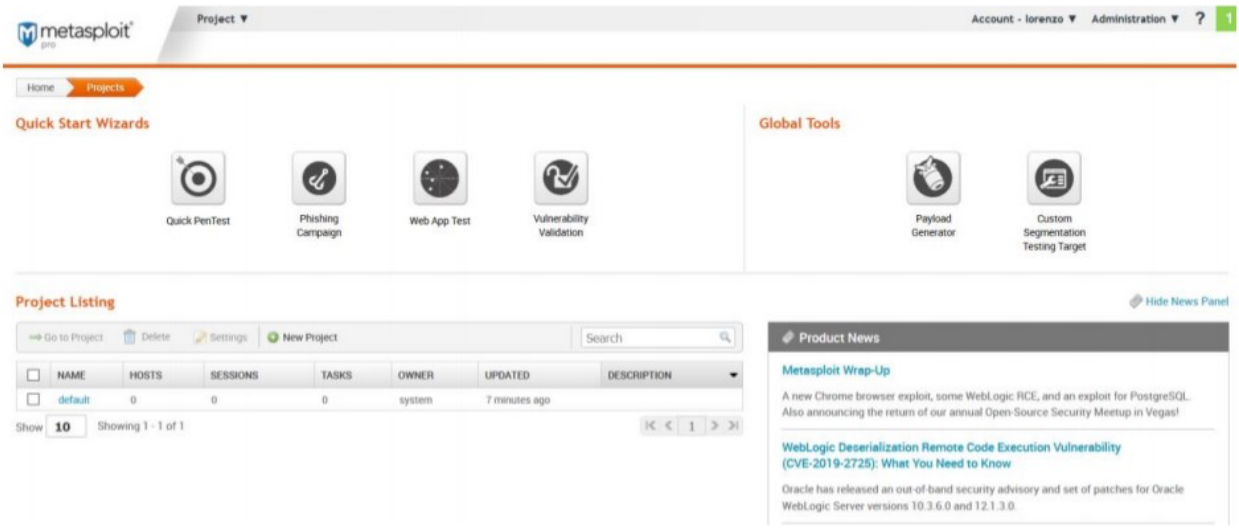


Рисунок 15 Веб-інтерфейс фреймворку Metasploit

Для виконання pentest використовуються спеціальні операційні системи. Kali, Linux - це відкритий код - дистрибутив, який містить попередньо встановлені інструменти для роботи з кібербезпеки. Metasploit, Nessus та інші пакети команд включені до нього. Parrot OS є альтернативою Kali, як також попередньо встановлено найрізноманітніші інструменти. Різниця полягає в основному в інтерфейсі робочого столу і обидві операційні системи можна завантажити безкоштовно.

Методики імітації

Методики імітації мають функцію спокусити зловмисників виконувати зловмисні операції , тобто імітувати не цінні ресурси компанії. Він складається з комп'ютера, що імітує послуги, які добровільно вразливі та привертають увагу потенційного зловмисника. Його мета - бути подібний до виробничого комп’ютера, так що хакер взаємодіє з ним. Раз хтось має виконавши сканування портів або спробувавши підключитися до нього, будь-яка дія буде реєструватися та контролюватися IDS для збору інформації про кібератаку. Це спосіб пізнання і розуміння методів, які

використовують хакери, але їх слід налаштовувати ретельно, щоб бути ефективними.

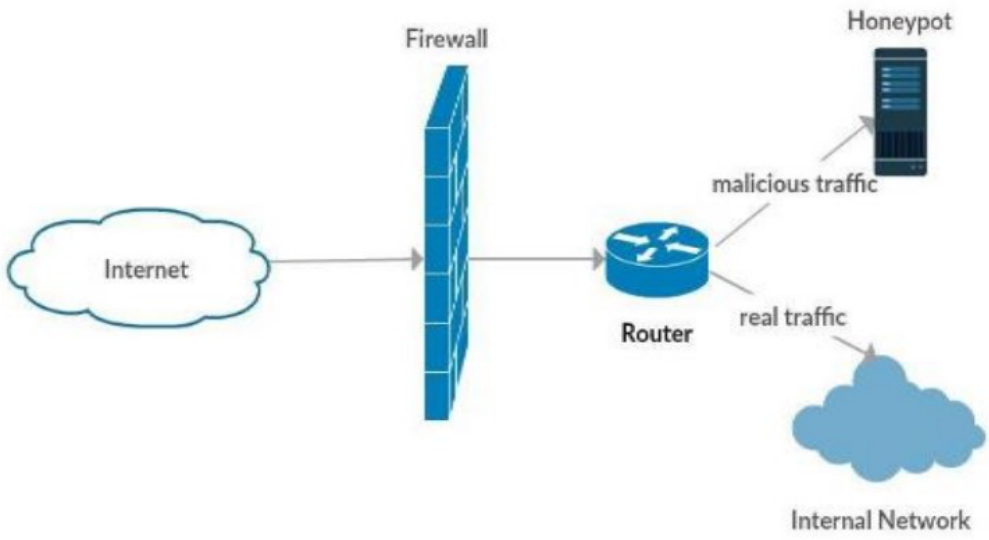


Рисунок 16 «Методика імітації (Honeypot)» у середовищі

Вразливі місця не повинні бути надто очевидними та надто простими для використання. Можна дивитись, скільки є доступної взаємодії у хакерів. Honeypot із низькою взаємодією буде лише імітувати запущені служби, відкриваючи порти. Інформація іметування надходить до телекомунікаційної системи про зловмисника, але це представляє менше ризиків, ніж дозволяючи більшу взаємодію у системі. Honeypot працює з високою взаємодією насправді та працює із вразливими службами, які призначені для цього, як зловмисники намагаються здійснити ескалацію привілеїв. Оскільки цей тип дозволяє хакерам заволодіти машиною, це повинні бути захищені сервери, а розповсюдження на решту телекомунікаційної мережі компанії необхідно заборонити. Методика імітації в основному використовуються великими компаніями, які мають необхідні знання для вивчення поведінки хакерів та не допускаючи помилок і не піддаючи всій компанії любий ризик.

У них також є бюджет на відтворення мережі апаратів для методики імітації, що називається honey net, що може бути ще більш привабливим для зловмисника та більш реалістичним.

Honeypot можна встановлювати на віртуальних машинах. Вони пропонують переваги перед апаратним забезпеченням, як легше відновлення у випадку пошкодження. Віртуальні машини також дешевші і більш безпечні, оскільки вони ізольовані від мережі.

5. РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ

5.1 Можливості запуску проекту

Ринок кібербезпеки вже коштує понад 100 мільярдів доларів - і, за прогнозами, він перевищить 300 мільярдів доларів до 2024 року. Не дивно, що безпека є однією з найгарячіших сфер інновацій та фінансування IT.

Коли десять років тому власників малого бізнесу запитували, що їх найбільше турбує, податки могли бути вгорі списку. Сьогодні загрози кібербезпеки зайняли перше місце в цьому списку проблем.

Відповідно до Звіту про вартість порушення даних за 2019 рік Інститутом Понемона / IBM Security, середня вартість порушення даних у США становить 3,92 млн. Доларів США, переважна більшість з яких (67%) реалізується протягом першого року порушення. . Що стосується бізнесу в Азіатсько-Тихоокеанському регіоні, Microsoft повідомляє, що кіберзлочинність може коштувати бізнесу 1,75 трлн. Дол. США , що призвело до втрати робочих місць у 67% фірм. Для більшості підприємств у всіх галузях промисловості найбільші витрати обумовлені втратою клієнтів після порушення даних. За підрахунками, втрата бізнесу становить 36% від загальної вартості порушення . Якщо цими цифрами все-таки потрібно обійтися, вам слід вжити активних заходів, щоб захистити свій бізнес від кіберзлочинців.

Метою даного розділу є створення інноваційного бачення, маркетинговий аналіз майбутніх здобутків при захисті бізнесу від цільових атак кіберзлочинців, спрямованих на крадіжку конфіденційних даних або відмову в обслуговуванні ваших сервісів, а також оцінка можливості введення у комерцію основних науково-технічних розробок, описаних в попередніх розділах магістерської дисертації шляхом розробки концепції стартап-проекту в умовах висококонкурентної ринкової економіки глобалізаційних процесів.

Проаналізовано та подано у вигляді таблиць:

- зміст ідеї;
- можливі напрямки застосування;
- основні вигоди, що може отримати користувач товару (за кожним напрямком застосування);
- чим відрізняють від існуючих аналогів та замінників.

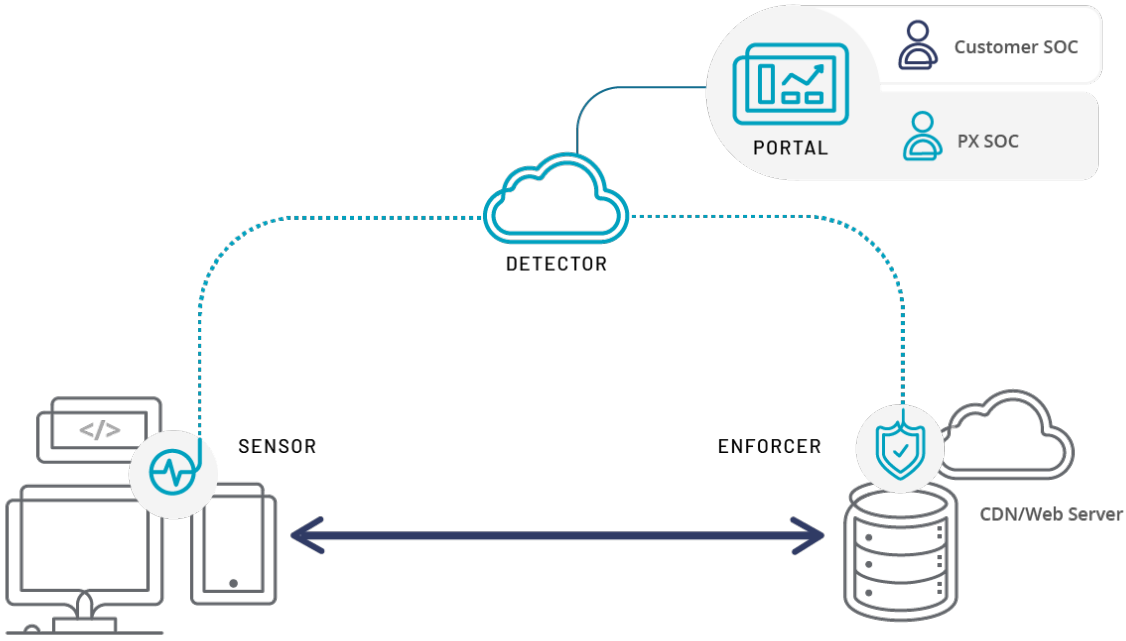
В таблиці 4.1 представлений опис ідеї стартап-проекту

Таблиця 4.1 Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Переваги
Захист від ботів	1. Захист від зловживань обліковим записом	Ефективність
	2. Захист від веб-скрапінгу	Надійність
	3. Захист від збирання данних	Простота застосування

Аналіз потенційних техніко-економічних переваг порівняно з пропозиціями конкурентів передбачає:

- визначення переліку техніко-економічних властивостей та характеристик;
- визначення попереднього кола конкурентів або товарів-замінників чи товарів-аналогів, що вже існують на ринку, та проведення збору інформації щодо значень техніко-економічних показників для ідеї власного проекту та проектів конкурентів.



В даний момент аналоги є, але не використовуються саме в цьому напрямку.

5.2 Технологічний аудит

В межах даного підрозділу проведено аудит технології, за допомогою якої можна реалізувати ідею проекту. Визначення технологічної здійсненності ідеї проекту передбачає аналіз таких складових (таблиця 4.2):

- за якою технологією буде виготовлено товар згідно ідеї проекту;
- чи існують такі технології чи їх потрібно розробити/допрацювати;
- чи доступні такі технології авторам проекту.

Таблиця 4.2 Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Захист від ботів у веб- та мобільних додатках API	Програмні засоби для планування проекту	Наявні	Доступно
		Спеціальне програмне забезпечення	Потребує розробки	Частково доступно

5.3 Розробка ринкової стратегії проекту

Визначення ринкових можливостей, які можна використати під час ринкового впровадження проекту, та ринкових загроз, які можуть перешкодити реалізації проекту, дає змогу спланувати напрями розвитку проекту із урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів-конкурентів. Спочатку проводять аналіз попиту: наявність попиту, обсяг, динаміка розвитку ринку (табл. 4.3).

Таблиця 4.3 Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1.	Кількість головних гравців, од	3
2.	Загальний обсяг продаж, грн/ум.од	12000000
3.	Динаміка ринку (якісна оцінка)	Зростає
4.	Наявність обмежень для входу (вказати характер обмежень)	Немає
5.	Специфічні вимоги до стандартизації та сертифікації	Є

№ п/п	Показники стану ринку (найменування)	Характеристика
6.	Середня норма рентабельності в галузі або по ринку,%	250%

Середня норма рентабельності в галузі (або по ринку) порівнюють із банківським відсотком на вкладення. За результатами попереднього оцінювання ринок є привабливим для входження.

Надалі визначають потенційні групи клієнтів, їх характеристики, та формують орієнтовний перелік вимог до товару для кожної групи (табл. 4.4).

Після визначення потенційних груп клієнтів проведений аналіз ринкового середовища: складені таблиці факторів, що сприяють ринковому впровадженню проекту, та факторів, що йому перешкоджають.

Таблиця 4.4 Характеристика потенційних клієнтів стартап-проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Конфіденційність даних	Веб додатки та API	Поведінку клієнта формують потреби; особливостей купівлі та експлуатації товару немає	Високий рівень та висока ефективність

Таблиця 4.5 Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1	Наявність кваліфікованих кадрів	Потрібні люди з високим досвідом роботи в сфері програмування API	Пошук кваліфікованого персоналу
2.	Потреба в ресурсах	Необхідні високі умови для технічної реалізації	Укладання договорів з комерційними організаціями

Надалі проведений аналіз пропозиції: визначені загальні риси конкуренції на ринку (табл. 4.6)

Таблиця 4.6 Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства
1. Олігополія	На ринку присутня невелика кількість фірм, які впроваджують захист від вебавтоматизації та збору конфеденційних данних	Підвищувати якість товару за рахунок використання передових технологій
2. За рівнем конкурентної боротьби міжнародний	Місцезнаходження фірм не обмежується територіально; офіси розміщено у різних країнах	Створювати веб-сайт компанії
3. За галузевою ознакою:внутріш ньогалузева	Економічна боротьба між різними товаровиробниками, які діють в одній галузі економіки.	Слідкувати за новітніми технологіями

На основі аналізу конкуренції, наведеного в табл. 4.7, а також із урахуванням характеристик ідеї проекту, вимог споживачів до товару визначено та обґрунтовано перелік факторів конкурентоспроможності. Аналіз оформлено у вигляді таблиці 4.7.

Таблиця 4.7 Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування
1.	Ступінь задоволення потреб користувача	Необхідно надати високоефективну, надійну систему
2.	Якість розробки з точки зору оптимальності показників надійності	Швидкодія та стабільність
3	Наявність наукових ресурсів	Необхідна наявність наукових кадрів з високим досвідом роботи
4	Економічний	Середня ціна продукту

За визначеними факторами конкурентоспроможності проводять аналіз сильних та слабких сторін стартап-проекту (таблиця 4.8).

Таблиця 4.8 Порівняльний аналіз сильних та слабких сторін проекту

№ п/п	Фактор конкурентоспроможності	Бали 1-20	-3	-2	-1	0	+1	+2	+3
1.	Ступінь задоволення потреб користувача	20							+
2.	Якість розробки з точки зору оптимальності показників надійності	20							+
3.	Наявність наукових ресурсів	20							+
4.	Економічний	20							+

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку: опис цільових груп потенційних споживачів (табл. 4.9).

Таблиця 4.9 Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1.	Розробники систем мобільних	Готові	Високий	Низька	Середня

	додатків				
2.	Веб-сайти з обліковими записами	Готові	Високий	Середня	Середня

Для роботи в обраних сегментах ринку сформовано базову стратегію розвитку (таблиця 4.10).

Таблиця 4.10 Визначення базової стратегії розвитку

№ п/п	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
1.	За рахунок великих можливостей по об’ємах збуту товарів	Витрати на виробництво	Стратегія лідерства на витратах
2.	Надання товару важливих з точки зору споживача відмітних властивостей, які роблять товар відмінним від товарів конкурентів.	Формування попиту якісним покриттям та швидкістю доступу до мережі	Стратегія диференціації

В результаті аналізу обираємо стратегію диференціації. Наступним кроком є вибір стратегії конкурентної поведінки (таблиця 4.11)

Таблиця 4.11 Визначення базової стратегії конкурентної поведінки

№ п/п	Чи є проект "першопрохідцем" на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки*
1.	Ні	Так	Ні	Стратегія «лідер»

Визначаємо стратегію позиціювання (таблиця 4.12)

Таблиця 4.12 Визначення стратегії позиціонування

№	Вимоги до	Базова	Ключові	Вибір асоціацій, які мають

п/п	товару цільової аудиторії	стратегія розвитку	конкурентоспроможні позиції власного стартап- проекту	сформувати комплексну позицію власного проекту (три ключових)
1.	Конфіденційність Захист від ботів у веб- та мобільних додатках API	Диференціації	Середня ціна, висока якість, доступність	Наукоємність, співпраця, ефективність

5.4 Розробка маркетингової програми

Визначення ключових переваг концепції потенційного товару представлене в таблиці 4.13.

Таблиця 4.13 Визначення ключових переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує технологія	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити
1.	Конфіденційність Захист від ботів у веб- та мобільних додатках API	Захист від зловживань обліковим записом (кардингу, оплати, веб-скрапінгу)	Підвищення захисту додатків Программа збирає та надсилає сотні індикаторів на стороні клієнта в Детектор для точного визначення людського трафіку проти активності ботів. Сигнали або індикатори використовуються для створення відбитків пальців пристрою та браузера.

Надалі розробляють трирівневу маркетингову модель товару: уточнюють ідею продукту та/або послуги, його фізичні складові, особливості процесу його надання (таблиця 4.14).

Таблиця 4.14 Опис трьох рівнів моделі товару

<table>
<tr><td>Рівні товару</td><td colspan="3">Сутність та складові</td></tr>
<tr><td>І. Товар за задумом</td><td colspan="3">Сенсорна мережа з застосування великих даних і концепцією Інтернету Речей</td></tr>
<tr><td rowspan="5">ІІ. Товар у реальному виконанні</td><td>Властивості/характеристики</td><td>М/Нм</td><td>Вр/Тх /Тл/Е/Ор</td></tr>
<tr><td>1. Низька ціна у порівнянні з конкурентами
2. Висока надійність
3. Ефективність</td><td>М

М
М</td><td></td></tr>
<tr><td colspan="3">Якість: стабільна робота та надійне покриття</td></tr>
<tr><td colspan="3">Пакування: -</td></tr>
<tr><td colspan="3">Марка: «БСМ»</td></tr>
<tr><td rowspan="2">ІІІ. Товар із підкріпленням</td><td colspan="3">До продажу гарантія</td></tr>
<tr><td colspan="3">Після продажу обслуговування, налаштування.</td></tr>
<tr><td colspan="4">За рахунок чого потенційний товар буде захищено від копіювання: захист інтелектуальної власності</td></tr>
</table>

Захист розробленого продукту буде регламентуватися як захист інтелектуальної власності товару.

Визначення меж встановлення ціни представлене у вигляді таблиці 4.15.

Таблиця 4.15 Визначення меж встановлення ціни

№ п/п	Рівень цін на товари-замінники	Рівень цін на товари- аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
1.	–	25млн…65млн грн	120млн грн. і вище	3,5 млн – 4,3млн грн.

Так як налаштування обладнання у кінцевого користувача потребує певних професійних навиків від персоналу і обладнання налаштовують під кожного клієнта індивідуально, то збут доцільно проводити власними силами без застосування посередників [50].

5.5 Висновки до розділу

1. Розроблено стартап-проект- рішення для керування ботами на основі поведінки, яке захищає ваші веб-сайти, мобільні додатки та API від автоматизованих атак, захищаючи ваш Інтернет-дохід, зменшуючи ризик порушення даних та покращуючи операційну ефективність.

2. Проведено аналіз потенційних техніко-економічних переваг порівняно з пропозиціями конкурентів. Визначено, що технологія переважає найближчих конкурентів в економічних та технологічних характеристиках.

3. Досліджено ринкові загрози та ринкові можливості, які складають на основі аналізу факторів загроз та факторів можливостей маркетингового середовища. Розроблено ринкову стратегію проекту та маркетингову програму стартап-проекту.

В результаті аналізу визначено, що верхня та нижня межі встановлення ціни на товар/послугу - 3,5млн – 4,3млн грн.

ВИСНОВКИ

Хакери використовують ті ж самі інструменти для виявлення вразливостей та експлуатації, як і IT- адміністратори телекомунікаційних систем. Особливо щодо безпеки великих телекомунікаційних систем компаній, ця гонка раніше знаходила тільки недоліки. Оскільки нові уразливості з'являються щодня, виправлення порушень у міру їх появи - це єдине, що можна зробити для захисту нульової вразливості, саме тому кібербезпека є "статичним рішенням динамічної проблеми". Немає впевненості, що наступного дня це буде здійснено розгорнутого і цього буде достатньо, але щось можна зробити зараз.

У хакерів може бути багато мотивів орієнтуватися на конкретну телекомунікаційну систему. Збір інформації про ціль за допомогою таких команд, як “Who is”, перший і найпростіший крок, який називається “слідом”. Потім зловмисник може сканувати наявність відкритих портів, виявляючи, якими послугами користується телекомунікаційна система та мережа, а також спробувати встановити зв’язки.

Серед найпоширеніших кібератак - це фішингові атаки найчастіші, оскільки вони прості у виконанні та можуть призвести до серйозних збитків. Експлуатування не виправлених компонентів з уразливостями та атакуючі бази даних із введенням SQL також дуже руйнівний і порівняно простий у виконанні. Зосередження уваги на типових атаках - хороший перший крок, але деякі телекомунікаційні системи повинні дотримуватися вказівок, таких як політика щодо паролів та фітинг сенсибілізація, для поліпшення їх безпеки. Технічні засоби, такі як брандмауери та антивіруси повинні бути впроваджені, а також є найкращі практики, такі як створення підмереж, які є ефективним рішенням.

Спеціалізовані компанії з кібербезпеки пропонують свої послуги іншим компаніям та допомагають їм в оцінкі ризиків та впровадження нових засобів захисту. В основному співпрацюють з великими системами, ці спеціалізовані підприємства є експертами у виявленні недоліків, оцінкі вразливості та тестування на проникнення. Робити ці операції вдома також можливо, оскільки деякі автоматизовані інструменти доступні на ринку.

За даною темою дослідження – ця магістерська робота містить загальний огляд існуючих кібератак та рекомендації для захисту від кібер атак. Дещо такі теми, як інструменти злому, можна розвивати ще далі, оскільки існує велика спільнота, яка працює над автоматизованими программами та програмним забезпеченням, які допомагають виконувати тести на проникнення. Світ кібербезпеки величезний і з кожним днем стає все більшим. Крім того, порівняння існуючих рішень може бути цікавим способом продовжити дану магістерську роботу. Існує безліч програм проти зловмисного програмного забезпечення, і всі вони не мають однакову продуктивність. Засоби оцінки вразливості та тестування на проникнення також варто порівняти та вивчаючи більш поглиблено.

Були виконані наступні задачі:

1. Виконано огляд літератури з теми дослідження. Розглянуті поняття з кібератак та кібер безпеки, досліджено основні сфери застосування;

2. Розглянуто методи застосування технологій кібератаки на телекомунікаційну мережу та методики її захисту від несанкціонованих атак;

3. Виконано розробку з захисту від кіберзагроз на телекомунікаційну мережу та рішення як себе захистити від кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. ISO/IEC 27000 family - Information security management systems. (n.d.). Retrieved from International Organization for Standardization: https://www.iso.org/isoiec-27001- information-security.html

2. ISO/IEC 27001:2013. (n.d.). Retrieved from ISO/IEC 27001: https://www.iso27001security.com/html/27001.html

3. Malwarebytes. (2019, April 2). Social engineering. Retrieved from Malwarebytes: https://blog.malwarebytes.com/glossary/social-engineering/ Managing malware. (n.d.). Retrieved from Accenture: https://www.accenture.com/usen/insight-managing-malware

4. Honeypot (computing). Retrieved from Techtarget: https://searchsecurity.techtarget.com/definition/honey-pot

5. Pentest (penetration testing) . Retrieved from Searchsecurity: https://searchsecurity.techtarget.com/definition/penetration-testing

6. Virtual honeypot. Retrieved from Techtarget: https://whatis.techtarget.com/definition/virtual-honeypot

7. Retrieved from OWASP Top 10 Security Risks – Part III: https://blog.sucuri.net/2018/12/owasp-top-10-security-risks-part-iii.html.
8. R. Shanmugavadivu, “Network Intrusion Detection System Using Fuzzy Logic,” *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 2, pp. 101–111, 2011

9. М. Г. Медведєв і І. О. Пащенко, *Теорія ймовірностей та математична статистика*, Київ, Ліра-К, 2008
10. М. В. Демчишин, Є. Г. Левченко і Д. І. Рабчун, «Графоаналітичний метод пошуку сідлової точки в ігрових задачах інформаційної безпеки*», Системні дослідження та інформаційні технології*, №3, сс.48–61, 2014
11. L. A. Gordon and M. P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp.438–457, 2002
12. H. I. Ansoff, *Strategic Management, UK : Palgrave Macmillan*, 2007. DOI: 10.1057/9780230590601
13. T. Moore, D. Pym and C. Ioannidis, *Economics of Information Security and Privacy*, US, Springer, 2010. DOI: 10.1007/978-1-4419-6967-5.
14. S. Goel and V. Chen, "Information Security Risk Analyses – a Matrix-Based Approach," in *Information Resource Management Association International Conference*, San Diego, USA, 2005
15. L. A. Zadeh, "Stochastic Finite-State Systems in Control Theory," *Information Sciences*, no. 251, pp. 1–9, 2013.
16. I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, "Choices for interaction with things on Internet and underlying issues," Ad Hoc Networks, vol. 28, pp. 68– 90, 2015.
17. J. P. Vasseur and A. Dunkels, "Ip for smart objects," White Paper 1, IPSO Alliance, 2008
18. P. Agrawal and S. Bhuraria, "Near field communication," SETLabs Bridfings, vol. 10, no. 1, pp. 67–74, 2012
19. B. Shanmuga Sundaram, "A quantitative analysis of 802.11ah wireless standard," International Journal of Latest Research in Engineering and Technology, vol. 2, 2016

20. W. Sun, M. Choi, and S. Choi, “Ieee 802.11 ah: a long range 802.11 wlan at sub 1 ghz,” Journal of ICT Standardization, vol. 1, no. 1, pp. 83–108, 2013
21. Zulkifli, M. Zaid W. Mohd, “Attack on Cryptography”, (2008)
22. P. I. Radoglou Grammatikis, P. G. Sarigiannidis, and I. D. Moscholios, “Securing the Internet of Things: Challenges, threats and solutions,” Internet of Things, vol. 5, pp. 41–70, Mar. 2019
23. J. Sengupta, S. Ruj, and S. Das Bit, “A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT,” Journal of Network and Computer Applications, vol. 149, p. 102481, Jan. 2020
24. S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” Computer Networks, vol. 76, pp. 146–164, Jan. 2015
25. K. S. Edge, G. C. Dalton, R. A. Raines, and R. F. Mills, “Using Attack and Protection Trees to Analyze Threats and Defenses to Homeland Security,” in MILCOM 2006 - 2006 IEEE Military Communications conference, 2006, pp. 1–7
26. J. Xu, W.-T. Zhu, and D.-G. Feng, “An improved smart card-based password authentication scheme with provable security,” Comput. Stand. Interfaces, vol. 31, no. 4, pp. 723–728, 2009
27. H. Šemić and S. Mrdovic, “IoT honeypot: A multi-component solution for handling manual and Mirai-based attacks,” in 2017 25th Telecommunications Forum, TELFOR 2017 - Proceedings, 2018
28. C. Anderson, “Docker [software engineering],” IEEE Software, vol. 32, no. 3, pp. 102–c3, 2015
29. Розроблення стартап-проекту [Електронний ресурс]: Методичні рекомендації до виконання розділу магістерських дисертацій для студентів інженерних спеціальностей/За заг. ред. О.А. Гавриша. – Київ: НТУУ «КПІ», 2016. – 28 с.

30. Д. І. Рабчун, «Оцінка ефективності інформаційної безпеки з урахуванням економічних показників»,
31. *Сучасний захист інформації*, №4, сс. 91–96, 2015
32. A. Platzer, *Logical Analysis of Hybrid Dynamical Systems: Proving Theorems for Complex Dynamics*, USA, Springer, 2010. DOI: 10.1007/978-3-642-14509-4
33. Є. Г. Левченко і А. О. Рабчун, «Оптимізаційні задачі менеджменту інформаційної безпеки», *Сучасний захист інформації*, №1 (1), сс. 16–24, 2010
34. В. В. Глушак і О. М. Новіков, «Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника», *Системні дослідження та інформаційні технології*, №2, сс. 89–100, 2013
35. В. В. Глушак і О. М. Новіков, «Метод проектування систем захисту інформації з використанням детермінованої гри „захисник-зловмисник“», *Наукові вісті НТУУ «КПІ»*, №2, сс. 46–53, 2011

УКРАЇНА

СВІДОЦТВО

про реєстрацію авторського права на твір

№ 79688

Науковий твір "Методологія захисту персональних даних в Wi-Fi мережах"

(вид, назва твору)

Автор(и) Єрмаков Антон Валерійович, Папушой Ольга Костянтинівна, Наратник Теодор Миколайович, Авдєєнко Гліб Леонідович, Тищенко Олена Петрівна, Постернак Богдан Сергійович, Клин Іван Миколайович, Середюк Дмитро Олександрович, Якорнов Євгеній Аркадійович, Цуканов Олег Федорович

(повне ім'я, псевдонім (за наявності))

Дата реєстрації 08.06.2018

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ ІДЕНТИФІКАЦІЙНИЙ КОД 37502596

М.П.

Державний секретар Міністерства економічного розвитку і торгівлі України О. Ю. Перевезенцев

Додаток 1 – Методологія захисту персональних даних в Wi-Fi мереж

УКРАЇНА

СВІДОЦТВО

про реєстрацію авторського права на твір

№ 76226

Науковий твір "Модель проектування бездротової мережі Wi-Fi на основі стандарту 802.11"

(вид, назва твору)

Автор(и) Єрмаков Антон Валерійович, Наритник Теодор Миколайович, Авдєєнко Гліб Леонідович, Вальчук Денис Сергійович, Бондарчук Сергій Олегович, Гошко Анастасія Павлівна, Середюк Дмитро Олександрович

(повне ім'я, псевдонім (за наявності))

Дата реєстрації 24.01.2018

Державний секретар Міністерства економічного розвитку і торгівлі України О. Ю. Перевезенцев

Додаток 2 – Модель проектування бездротової мережі Wi-Fi на основі стандарту 802.11

УКРАЇНА

СВІДОЦТВО

про реєстрацію авторського права на твір

№ 76224

Науковий твір "Декомпозиція методів захисту мережі передачі даних від перевантажень."

(вид, назва твору)

Автор(и) Єрмаков Антон Валерійович, Наритник Теодор Миколайович, Авдєєнко Гліб Леонідович, Мозговий Сергій Олександрович, Папушой Ольга Костянтинівна, Тимченко Сергій Анатолійович, Середюк Дмитро Олександрович

(повне ім'я, псевдонім (за наявності))

Дата реєстрації 24.01.2018

Міністерство економічного розвитку і торгівлі України ідентифікаційний код 37508596

Державний секретар Міністерства економічного розвитку і торгівлі України О. Ю. Перевезенцев

Додаток 3 – Декомпозиція методів захисту мережі передачі даних від перевантажень

УКРАЇНА

СВІДОЦТВО

про реєстрацію авторського права на твір

№ 76225

Науковий твір "Методика оцінювання систем підтримки мобільності для мереж 4-го покоління з малими стільниками"

(вид, назва твору)

Автор(и) Єрмаков Антон Валерійович, Наритник Теодор Миколайович, Авдєєнко Гліб Леонідович, Мозговий Сергій Олександрович, Папушой Ольга Костянтинівна, Кравець Олександра Олександрівна, Середюк Дмитро Олександрович

(повне ім'я, псевдонім (за наявності))

Дата реєстрації 24.01.2018

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ ІДЕНТИФІКАЦІЙНИЙ КОД 37508596

Державний секретар Міністерства економічного розвитку і торгівлі України О. Ю. Перевезенцев

Додаток 4 – Методика оцінювання систем підтримки мобільності для мереж 4-го покоління з малими стільниками

УКРАЇНА

СВІДОЦТВО

про реєстрацію авторського права на твір

№ 76214

Науковий твір "Трансляція радіосигналів цифрового телебачення стандарту DVB-C по наземному радіоканалу НВЧ-діапазону"

(вид, назва твору)

Автор(и) Єрмаков Антон Валерійович, Наритник Теодор Миколайович, Авдєєнко Гліб Леонідович, Якорнов Євгеній Аркадійович, Цуканов Олег Федорович, Клин Іван Максимович, Сердюк Дмитро Олександрович

(повне ім'я, псевдонім (за наявності))

Дата реєстрації 24.01.2018

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ ІДЕНТИФІКАЦІЙНИЙ КОД 37508596

Державний секретар Міністерства економічного розвитку і торгівлі України О. Ю. Перевезенцев

Додаток 5 – Трансляція радіосигналів цифрового телебачення стандарту DVB-C по наземному радіоканалу НВЧ-діапазону

УКРАЇНА

СВІДОЦТВО

про реєстрацію авторського права на твір

№ 76223

Науковий твір "Метод оптимізації антени супутникового ретранслятора для досягнення умов узгодження координації з іноземними адміністраціями"

(вид, назва твору)

Автор(и) Єрмаков Антон Валерійович, Наритник Теодор Миколайович, Авдєєнко Гліб Леонідович, Вальчук Денис Сергійович, Бондарчук Сергій Олегович, Кравець Олександра Олександрівна, Середюк Дмитро Олександрович

(повне ім'я, псевдонім (за наявності))

Дата реєстрації 24.01.2018

Міністерство економічного розвитку і торгівлі України Ідентифікаційний код 37508596

Державний секретар Міністерства економічного розвитку і торгівлі України О. Ю. Перевезенцев

Додаток 6 – Метод оптимізації антені супутникового ретранслятора для досягнення умов узгодження координації з іноземними адміністраціями