Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Методи захисту корпоративної пошти від кібератак за допомогою сканерів пошти»

Виконавець: студент IV курсу, групи КБ-41

_____ **Даніїл ТИХОМИРОВ**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник	Сергій ДАКОВ	

Нормоконтроль	Юрій ЩЕБЛАНІН	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідуюча кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-41** (група) **Тихомирову Даніїлу Євгенійовичу** (прізвище ім'я по батькові)

Тема дипломної роботи Методи захисту корпоративної пошти від кібератак за допомогою сканерів пошти

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Поштовий сервер, сніфери, мережеві протоколи, мережеві сканери, файєрвол

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Нормативно-правова база про захист інформації, мережеві протоколи, поштовий сервер, загрози для корп. пошту

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Забезпечення захисту копроративної пошти в організаціях

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 01 листопада 2021 року

Завдання видав _____ Сергій ДАКОВ
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Данiїл ТИХОМИРОВ
(підпис) (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2021 – 26.01.2022	*виконано*
2	Аналіз літератури	27.01.2022 – 20.02.2022	*виконано*
3	Аналіз потенційних загроз для корпоративної пошти	21.02.2022 – 03.03.2022	*виконано*
4	Дослідження типів мережевих атак	04.03.2022 – 30.03.2022	*виконано*
5	Аналіз засобів захисту корпоративної пошти	31.03.2022 – 17.04.2022	*виконано*
6	Конфігурація поштового сервера	18.04.2022 – 07.05.2022	*виконано*
7	Створення порівняльної таблиці	08.05.2022 – 26.05.2022	*виконано*
8	Оформлення пояснювальної записки	27.05.2022 – 05.06.2022	*виконано*
9	Підготовка до захисту	06.06.2022 –13.06.2022	*виконано*

Завдання видав _____ Сергій ДАКОВ
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Данеїл ТИХОМИРОВ
(підпис) (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 55 сторінок, включає в себе зміст, вступ, три розділи дипломної роботи, висновки та список джерел. У пояснювальній записці дипломної роботи міститься 8 рисунків та 3 таблиці

Метою роботи є розробка рекомендацій захисту корпоративної пошти від кібератак на базі методів сканування пошти

Для досягнення зазначеної мети поставлено наступні завдання:

- дослідити структуру поштового серверу та проаналізувати можливі атаки
- створити механізми виявлення шкідливого програмного забезпечення, спаму та фішингу в корпоративних поштах
- розробка рекомендацій захисту корпоративної пошти від кібератак за допомогою сканерів пошти

Методи дослідження дипломної роботи:

- аналітичні методи;
- системний підхід;
- методи порівняння;
- структурний аналіз

Об'єктом дослідження є процес захисту корпоративних пошти від кібератак

Предметом дослідження є засоби та механізми, які реалізують захист корпоративної пошти

Практичною цінністю розробленні рекомендації захисту корпоративних пошти від кібератак

Ключові слова: кібератака, захист інформації, виявлення шкідливого коду, запобігання спаму, поштовий сервер, мережева безпека

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ПЗ	–	Програмне забезпечення
ІС	–	Інформаційна Система
ITU	–	International Telecommunication Union
DDoS	–	Distributed Denial-of-service
ОЗП	–	Оперативне записуючий пристрій
DOS	–	Denial of Service
SSH	–	Secure Shell
TSL	–	Transport Layer Securit
TCP	–	Transmission Control Protocol
UDP	–	User Datagram Protocol
HTTP	–	Hypertext Transfer Protocol
ICMP	–	Internet Control Message Protocol
IMAP	–	Internet Message Access Protocol
IP	–	Internet Protocol
POP3	–	Post Office Protocol
SNMP	–	Simple Network Management Protocol
NAT	–	Network Address Translation

ЗМІСТ

ВСТУП

Актуальність дослідження. Модерне суспільство – це суспільство інформаційних технологій, що ґрунтується на щоденному використанні комп'ютерної техніки, мереж зв'язку, мобільних засобів спілкування та інших технічних засобів. Поточна робота державних структур, транспортної, енергетичної, банківської та інших систем нездійснима без безпечної роботи комп'ютерної техніки та способів комунікацій. Інформаційні технології стали стабільним супутником сьогочасної людини не тільки на робочому місці, вони проникнули майже в усі сфери людського життя.

Поширення сучасних інформаційних технологій, в основі яких лежить широке вживання комп'ютерної техніки та способів комунікацій, автоматизації та оптимізації процесів в усіх без виключення галузях життєдіяльності, спричинило до нівелювання меж та переплетення національних господарств та національних інфраструктур країн світу. Банківська система України є однією з галузей, де найбільш широко та активно використовуються новітні можливості інформаційних технологій та мережі Інтернет.

А зважаючи, що зазначені технології використовуються для грошових переказів, вказана сфера привертає все більшу увагу злочинців. Несанкціоноване списання грошових коштів з банківських рахунків, розповсюдження комп'ютерних вірусів, шахрайство з платіжними картками, DDoS атаки на Інтернет-ресурси, втручання в роботу Інтернет-банкінгу, шахрайство в інформаційних мережах – це не повний перелік кіберзлочинів, тобто злочинів у галузі комп'ютерних та інформаційних технологій. Актуальність теми дослідження полягає у відсутності чіткої та злагодженої системи заходів для вчасного виявлення фінансових операцій, що можуть бути пов'язані з відмиванням доходів, отриманих у галузі кіберзлочинності в Україні.

Вищевказані прерогативи даного виду злочину поряд з його значною прибутковістю стали безсумнівно істотними перевагами у порівнянні з іншими

злочинами, скоєння яких в умовах покращання правоохоронних систем стає все вартіснішим й важчим. Таким чином, проведення дослідження щодо основних схем та засобів відмивання доходів, отриманих у сфері кіберзлочинності, на сьогодні є актуальним та необхідним.

Метою роботи є реалізація засобів та механізмів захисту корпоративної пошти від спаму та фішингу

Об'єктом дослідження є процес захисту корпоративних пошти від спаму та фішингу

Предметом дослідження є засоби та механізми, які реалізують корпоративної пошти від спаму та фішингу

Методи дослідження дипломної роботи:

- аналіз літератури;
- аналіз документів;
- системний підхід;
- методи порівняння;
- структурний аналіз

Для досягнення зазначеної мети поставлено наступні завдання:

- дослідити структуру поштового серверу та проаналізувати можливі атаки
- проаналізувати засоби та механізми виявлення шкідливого програмного забезпечення, спаму та фішингу в корпоративних поштах
- впровадити та зконфігурувати систему захисту корпоративної пошти від спаму та шкідливого ПЗ

Практичною цінністю отриманих результатів є аналіз та практичне застосування систем захисту корпоративної пошти від спаму, фішингу та шкідливого ПЗ, яке в майбутньому може бути вдосконалене

Ключові слова: кібератака, захист інформації, виявлення шкідливого коду, запобігання спаму, поштовий сервер, мережева безпека

РОЗДІЛ 1
ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ КОРПОРАТИВНОЇ ПОШТИ ВІД КІБЕРАТАК

1.1 Оцінювання програми безпеки інформаційних систем

Одним із ключових елементів розвитку сучасного суспільства є все більший акцент на якості та надійності комп'ютерів, які використовуються в різних видах діяльності людини. Акцент слід зробити на напрямі діяльності ЗМІ, що вимагає підвищених вимог до їх безпеки. Проблема ускладнюється тим, що велика кількість IP-адресів мають найсильніший у світі доступ до Інтернету, а використання загальнодоступного програмного забезпечення призводить до незначної кількості випадкових і несподіваних атак на систему [1, с.16-18].

Зазначимо, що IP-адреси на базі Інтернет розглядаються для необхідності захисту системних активів від кібератак при реалізації технології доступу, зберігання, відправлення, обробки та передачі інформації. Сьогодні ідея кібербулінгу пояснює реалізацію загроз безпеці контенту (особливо конфіденційності, цілісності та доступності) у соціальних мережах з урахуванням їх слабких сторін [30]. У той же час кіберпростір – це час взаємодії користувачів, програмного забезпечення та інструментів, мережевих технологій для підтримки та управління інформаційним обміном для інтеграції соціальної інформації [2, с.61-64].

Пошук способу боротьби зі злочинністю за допомогою інформації та комунікації є центром уваги міжнародної спільноти, особливо української влади. Враховуючи, що технології розвиваються швидше, ніж приватні правила, і що кіберзлочинці незаконно імпортують гроші, важливо шукати нові рішення в таких сферах, як перетин кордонів. інформаційна безпека, захист інформації та правоохоронні послуги між приватним сектором та державними установами.

У зв’язку з потенційним впливом цієї кризи міжнародне співтовариство шукає надійних заходів для зменшення загрози злочинності проти суспільства. Протягом багатьох років було ратифіковано низку регіональних та міжнародних законів про технологічні злочини, включаючи запропоновані закони та закони про їх невідповідність.

Сьогодні Будапештська конвенція є наріжним каменем правового розвитку в боротьбі з технологічною злочинністю як на міжнародному рівні, так і окремо.

Будапештська угода закликає уряд:

- Удосконалення правил, які дозволяють компетентним органам ефективно розслідувати кіберзлочини та зберігати електронні докази, включаючи збір даних у режимі реального часу, онлайн-зберігання та публікацію інформації про дорожній рух, онлайн-зберігання, комп'ютерний захоплення та вилучення. комп'ютерна інформація, зміст бази даних;

- атаки на комп’ютерну систему та інформацію (тобто використання обладнання, незаконне володіння, незаконний доступ, перешкоджання інформації, доступ до системи), а також комп’ютерні правопорушення (шахрайство та підробка), правопорушення (порнографія) «дітей») та порушення прав і суміжних прав. ;

- розширення міжнародного співробітництва з іншими Договірними державами за допомогою загальних (взаємодопомога, експорт, добровільний обмін інформацією) та спеціальних заходів (взаємодопомога в доступі до комп'ютерної інформації, поширення та швидкого зберігання інформації, що зберігається в інформації, співробітництво). - перетин кордонів комп'ютерних даних, годинникової мережі). Конвенція про ліквідацію всіх форм дискримінації щодо жінок (T-CY) була створена, щоб допомогти країнам оцінити та обмінятися думками щодо необхідності внесення змін або протоколів до Конвенції.

Крім того, у 2006 р. Рада Європи започаткувала Міжнародний комітет з ліквідації всіх форм жорстокого, нелюдського чи такого, що принижує гідність, поводження чи покарання у приватному секторі, а також із захисту дітей від насильства та сексуального зловживання [3, с. 327].

Європейське поліцейське відомство (Європол) розпочало серію антикібератак. Сьогодні Європол надає аналітичну та слідчу допомогу членам ЄС через статистику злочинності та системи онлайн-нагляду. У 2013 році Європол запустив новий Європейський центр злочинності. Основна увага приділяється розслідуванню кібершахрайства, наприклад, боротьба з сексуальним насильством над дітьми через Інтернет, електронний банкінг та інші фінансові заходи, а також розслідування інших порушень безпеки Європейського Союзу та головної інфраструктури. Помітну роль у подоланні проблем міжнародної співпраці у сфері боротьби з кіберзлочинністю відіграє ООН, котра приділяє велику увагу проблемам поширення злочинів, пов’язаних з використання комп’ютерних та інформаційних систем, та боротьби з таким злочинами.

Організація Об’єднаних Націй неодноразово наголошувала на необхідності міжнародного співробітництва у запобіганні та розслідуванні злочинів проти людства. У 2011 році Управління ООН з наркотиків і злочинності та Міжнародний союз телекомунікацій підписали Конвенцію про ліквідацію всіх форм дискримінації щодо жінок (МТКЮ). Міжнародний союз електрозв'язку (МСЕ) був створений як Спеціальний доповідач Організації Об'єднаних Націй з питань зменшення тероризму та інформаційної безпеки: екологічні керівні принципи; методичні рекомендації щодо захисту дітей у навколишньому середовищі; Інструкції для батьків, опікунів та вчителів щодо захисту дітей в Інтернеті; Керівництво для Агентства з охорони навколишнього середовища; Global Internet Security Program [4, с.54-58].

Експерти Управління ООН з наркотиків і злочинності (UNODC) також кажуть, що міжнародне співробітництво включає правову допомогу, експорт, легалізацію міжнародних справ і незаконну співпрацю між правоохоронними органами. Крім того, зміна характеру електронних доказів у контексті міжнародного співробітництва у сфері кримінального судочинства вимагає відповідної реакції та можливості запитувати конкретні слідчі дії, наприклад, комп’ютерне зберігання.

На національному рівні профілактика злочинності складається із стратегій і стратегій, спрямованих на пом’якшення потенційної шкоди суспільству та особистості та зниження ризику злочинності. Стратегії запобігання кіберзлочинності включають нарощування потенціалу для кримінального правосуддя та правоохоронних органів, стратегію, законодавство про боротьбу з кіберзлочинністю, створення міцних знань та співпраці між урядами, належне управління, охоплення громадами, громадою, приватним сектором та міжнародною спільнотою.

На сьогодні законодавство України не визначає поняття «кіберзлочинність» чи «кіберзлочинність», а лише загальне визначення злочинів та правопорушень, вчинених з використанням комп’ютерних систем, комп’ютерів та телекомунікаційних мереж (глава XVI Кримінального кодексу України (далі – Кримінальний кодекс). Україна) зокрема [6]:

- створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 3611 КК України);

- несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку (стаття 361 КК України);

- несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації (стаття 3612 КК України); - порушення правил експлуатації електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку або порядку чи правил захисту інформації, яка в них оброблюється (стаття 363 КК України);

- несанкціоновані дії з інформацією, яка оброблюється в електроннообчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (стаття 362 КК України);

- перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (стаття 3631 КК України). Крім того, діяльність кіберзлочинців кваліфікується за статтею 200 КК України – незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення.

Експерти Управління ООН з ліквідації всіх форм дискримінації жінок і жінок у сфері наркотиків і наркотиків кажуть, що визначення «кіберзлочинності» багато в чому ґрунтується на призначенні цього терміну. Злочин ґрунтується на невеликій кількості дій проти приватності, конфіденційності та комп'ютерної чи інформаційної системи.

Загалом поняття інформаційної безпеки означає, що держава захищає фундаментальні інтереси особи, суспільства і держави, уникаючи наслідків: неповноти, своєчасності та недостовірності використовуваної інформації; несприятливий вплив інформації; негативні наслідки використання технологій; несанкціоноване поширення, використання, порушення приватності, конфіденційності та доступу до інформації [13, 217]. Крім того, поняття інформаційної безпеки (інформаційної безпеки) відноситься до того факту, що інформація підтверджує відповідність активам політики безпеки [5].

Водночас поняття інформаційної безпеки в інформаційній системі визначає діяльність, спрямовану на захист інформації, що обробляється ІБ та ІВ загалом, та запобігає або ускладнює терористичний потенціал, а також зменшує потенційні втрати від тероризму. Визначаючи безпеку продуктивності, зосередження на покращенні продуктивності та надійності значною мірою обумовлено ненавмисними пошкодженнями, несправностями, увагою до деталей і характером елемента, відмінність, яка вказує на несправність, - добре відома.

Незважаючи на це, володіти ним усе ще не під силу пересічній людині. Висновок ґрунтується на досвіді поширення критеріїв оцінки, затверджених у [39], де виявляється, що рівень незахищеності обладнання системи визначається

рівнем відповідності системи захисту та хорошою роботою. такий підхід реалізується. Зазначається, що відсутність захисту та невиконання заходів визначає слабкі сторони обладнання системи. Розповсюдження предметів було навмисно порушено, і про нещасний випадок не повідомлялося [6].

Крім того, [7] він використовує інформацію про інформаційну безпеку, що включає захист інформації навмисно чи навмисно за допомогою мистецтва чи природи. Крім того, зарубіжні книги з оцінки інформаційної безпеки [8, с.112-115] мають вимоги до безпеки. Тому, хоча це не зрозуміло в нинішньому контексті, можна припустити, що система моніторингу IP була зменшена для визначення цінності заходів безпеки, які вказують на наявність кібератак. У цьому випадку ідея встановлення стандартів безпеки буде інтерпретуватися як перелік індикаторів безпеки IP-безпеки.

В загальному випадку множина ПБ Інтерент-орієнтоваих ІС формуються на основі аналізу:

– параметрів вхідних та вихідних мережевих з’єднань по різноманітним протоколам;

– потенційно небезпечного програмного коду, який передається в ІС;

– параметрів, що відображають функціонування системного та прикладного програмного забезпечення ІС;

– функціональні параметри апаратного забезпечення ІС;

– параметри, що характеризують зміст інформації, котра передається в ІС.

Джерелом даних для встановлення ПБ є: операційна система операційної системи, на якій працює IP-сервер, база даних обладнання інформаційної безпеки (брандмауер, антивірус, система захисту від спаму, DLP-система), а також. Інструментарій кібератак 99). Ми перевіряємо РВ на предмет кібератак на основі IP. Зауважимо, що основна увага приділяється загальним планам ІВ, які широко використовуються в управлінні бізнесом, промисловістю та економікою [9, с.136-140].

Відповідно [1, 2], характерними властивостями Інтернет-орієнтованих ІС являються:

– підтримка типових Інтернет-сервісів (веб-сайту, електронної пошти),

– складність опису (досить велика кількість функцій, процесів, елементів даних і складні взаємозв'язки між ними);

– різнорідність методів та моделей, використаних при побудові її компонентів;

– наявність сукупності тісно взаємодіючих компонентів (підсистем), що мають свої локальні задачі й цілі функціонування (наприклад, традиційних додатків, пов'язаних з обробкою транзакцій і рішенням регламентних задач, і додатків аналітичної обробки (підтримки прийняття рішень), що використовують нерегламентовані запити до даних великого об'єму;

– функціонування в неоднорідному середовищі на декількох апаратнопрограмних платформах;

– необхідність постійної інтеграції в ІС існуючого і новоствореного програмного забезпечення;

– використання програмного забезпечення, створеного роз'єднаними і різнорідними групами розробників з різним рівнем кваліфікації і традиціями використання тих або інших інструментальних засобів;

– використання програмного забезпечення, яке в багатьох випадках не має офіційної підтримки та несе в собі потенційну загрозу безпеці за рахунок помилок, та люків, які можуть проявлятись тільки в певних умовах експлуатації;

– широке використання в програмного забезпечення архітектури розподілених об’єктів;

– складності адміністрування як в штатних умовах експлуатації, так і при модифікації програмного забезпечення;

– формування управлінських рекомендацій на основі обробки великих обсягів різнорідної інформації;

– необхідність постійної актуалізації інформаційних ресурсів;

– тісна інтегрованість з іншими Інтернет-орієнтованими ІС, частина з яких несуть в собі потенційні загрози як навмисного, так і ненавмиснго характеру;

– тісна взаємодія з зовнішнім Інтернет-середовищем, яке включає в себе велику кількість інформаційно-програмних деструктивних засобів;

– стандартизація та уніфікація процедур взаємодії між різними функціональними блоками ІС;

– інтелектуалізація процедур обробки даних, що значно ускладнює оцінювання управляючих сигналів ІС;

– адаптованість до користувачів з різною кваліфікацією, що значно зменшує ефективність захисту від деструктивних впливів;

– взаємодією з віддаленими користувачами;

– децентралізованість управління як системою захисту, так і всією ІС в 20 цілому, що в багатьох випадках визначає запізнення та зменшення ефективності управлінських впливів [10, с.139-147].

Простір цих властивостей показує, що основними факторами, що визначають особливості оцінки вітчизняних Інтернет-орієнтованих ІС ПБ, є:

– складність розпізнавання кібератак внаслідок складності встановлення явного зв’язку між порушенням інформаційної безпеки і певним видом кібератак, складністю визначення вразливостей програмного забезпечення та наслідків реалізації кібератак, можливістю виникнення порушення інформаційної безпеки без явно вираженої кібератаки, високої різноваріантності кібератак;

– виникнення нових видів кібератак по причині постійного вдосконалення методів та засобів здійснення кібератак, використання нових Інтернет-сервісів [1, 19, 59],

– необхідність функціонування при обмежених обчислювальних ресурсах, спричинених використанням бюджетного апаратного забезпечення та розташування на одній апаратній платформі Інтернет-серверів разом з СЗІ [2, 63, 66, 8],

– варіативність умов застосування, що обумовлюється реконфігурацією ІС, зміною програмно-апаратного забезпечення об’єктів ІС, модифікацією Інтернетсервісів, кваліфікацією адміністративного персоналу та ін. При цьому

результати [11, с.115-119] вказують на те, що типові порушення захищеності Інтернет-орієнтованих ІС виникають по причині деструктивного впливу:

– ШПЗ, розміщеного на веб-сторінках;

– ШПЗ, яке розповсюджується за допомогою електронної пошти; – витоків текстової інформації з використанням засобів електронної пошти; – нецільових електронних листів (спаму);

– віддалених мережевих кібератак на Інтернет-сервери. Наслідками деструктивних впливів може бути як порушення інформаційної безпеки типових Інтернет-сервісів, так і порушення інформаційної безпеки всіх інших функціональних блоків ІС.

1.2 Особливості формування методів захисту корпоративної пошти від кібератак за допомогою сканерів пошти

Сніффери (sniffers) - це програми, здатні перехоплювати і аналізувати мережевий трафік. Сніффери корисні в тих випадках, коли потрібно отримати з потоку даних будь-які відомості (наприклад, паролі) або провести діагностику мережі. Програму можна встановити на одному пристрої, до якого є доступ, і протягом короткого часу отримати всі дані, що передаються.

Принцип роботи Сніффера. Зупиніть трафік через сніфер, виконавши такі дії:

- на слух у звичайний спосіб,
- розрив координації,
- управління дорогами,
- за допомогою аналізу електромагнітного випромінювання,
- атакуючи мережу та рівень, він змінює мережеві шляхи.

Потік даних, захоплений Sniper, аналізується, що дозволяє:

- виявлення паразитного трафіку (його наявність значно збільшує навантаження на мережеве обладнання)

- Виявлення шкідливих і небажаних програм (мережевих сканерів, троянів, флоперів, пілінг-клієнтів тощо)

- Захоплюйте будь-який зашифрований або незашифрований трафік користувача для отримання паролів та інших цінних даних.

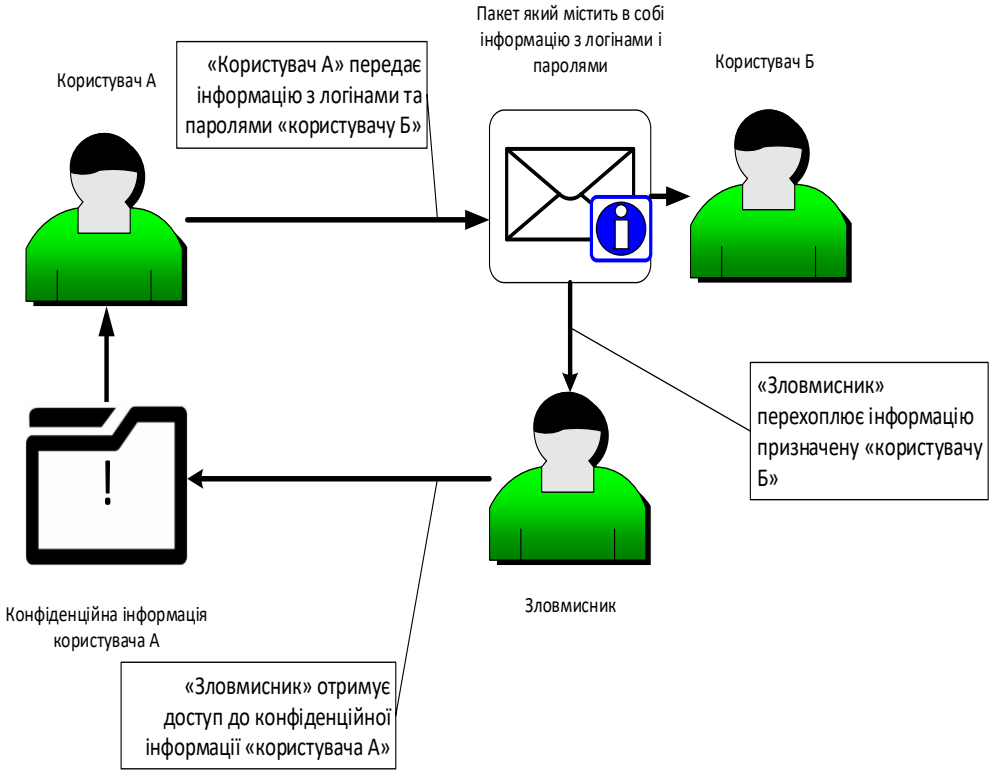

Рисунок 1.1 - Перехоплений потік даних за допомогою програми Wireshark

Таблиця 1.2

Аналіз типу атаки "Sniffer"

Алгоритм	Тип атаки: «Sniffing»
мета атаки	Виявити зміст службових заголовків, виявити паролі і ідентифікатори користувачів і т.п.
джерело загрози	внутрішнє, зовнішнє.
вразливість, що використовується при реалізації	Вразливість протоколів міжмережної взаємодії, порушнику необхідно пройти процедуру ідентифікації (по імені) і автентифікації (по паролю).
програми, які можуть застосовуватися при реалізації атаки	Програми перехоплення мережевих пакетів «сніфери» (Arpspoof, Urlsnarf, Dsniff)
об’єкт атаки	Мережевий трафік.
типові заходи захисту	Шифрування даних, Використання електронно-цифрового підпису (ЕЦП), Застосування антісніфферов, Застосування захищених каналів передачі даних - VPN, SSL / TLS, SSH, HTTPS.

Розгортання відмови в обслуговуванні, або DDoS, є справжнім вибухом на стороні сервера з одночасними вимогами. Атаки посилають ці вимоги до багатьох зламаних систем. Таким чином він намагається заволодіти Інтернетом і втратити оперативну пам’ять сім’ї жертви. Основна мета – закрити систему компанії та зупинити бізнес.

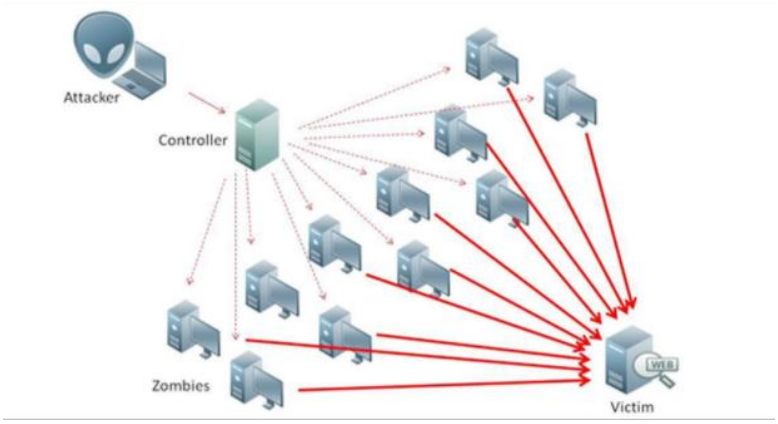

Рисунок 1.2 - Типова атака на "відмову в обслуговуванні"

Захист організації від DDoS-атак - це важлива частина стратегії по забезпеченню безпеки мережі. Щоб укрити мережу від атак по безлічі напрямків, необхідно розгорнути комплексну і цілісну IT-середовище, компоненти якої будуть працювати як єдине ціле.

Таблиця 1.3

Аналіз типу атаки "DDoS"

Алгоритм	**Тип атаки: DDoS-атака**
мета атаки	Порушення правильного функціонування вузла мережі.
джерело загрози	зовнішнє.
вразливість, що використовується при реалізації	Вразливість, обумовлена обмеженою пропускною спроможністю комп'ютера.
програми, які можуть застосовуватися при реалізації атаки	Утиліта Ping (Packet Internet Groper), File2ban, та інші.
об’єкт атаки	Хост (вузол) мережі
типові заходи захисту	Відключення відповіді на запити ICMP, Застосування засобів виявлення і запобігання вторгнень (IDPS), Застосування універсальних шлюзів безпеки, Обмеження обсягу трафіку, Блокування певних протоколів.

IP-спуфинг це відбувається, коли напад всередині або поза сім'єю імітує законного роботодавця. Це можна зробити двома способами. По-перше, зловмисник може використовувати IP-адресу, яка є частиною дійсної IP-адреси, або дійсну адресу, яка дозволяє отримати доступ до певного рядка.

Атаки IP-спуфінга пора кинути її і рухатися далі. Хорошим прикладом є DoS-атака, яка починається з іншої адреси, приховуючи точну особу зловмисника. Зазвичай розшифровка IP обмежується введенням неправильної інформації або шкідливих правил у звичайний спосіб передачі інформації між клієнтом і сервером або через лінію однорангового з'єднання. Для обох типів зв'язку хакер повинен змінити всі таблиці, щоб показати трафік на неправильну IP-адресу. Деякі з нападників, однак, навіть не намагалися знайти вирішення вимог. Якщо основним завданням є доступ до основного файлу в системі, результати роботи програми значення не мають.

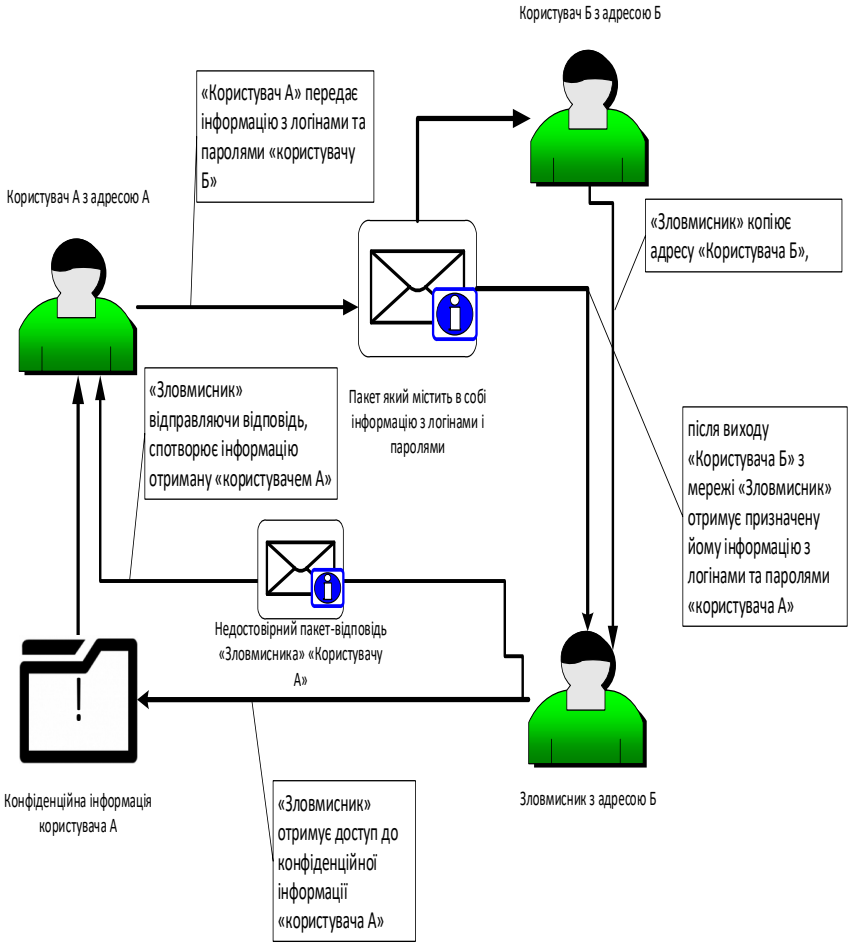

Рисунок 1.3 - Перехоплення інформації використовуючи IP-спуфінг

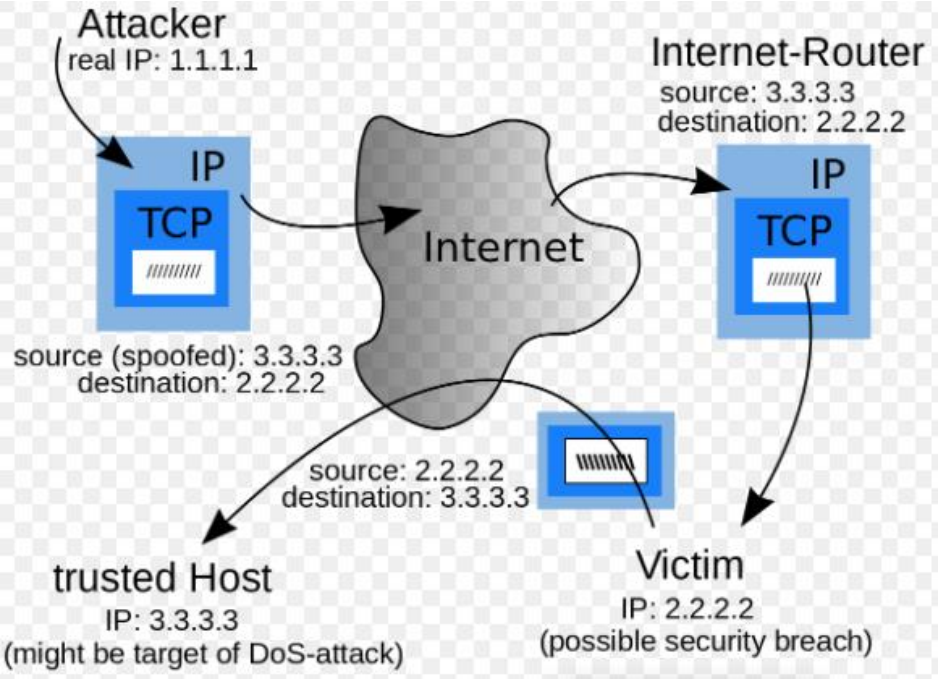

Рисунок 1.4 - Перенаправлення трафіку на помилкову IP-адресу

Таблиця 1.4

Аналіз типу атаки "IP - Spoofing"

Алгоритм	Тип атаки: «IP - спуфінг»
мета атаки	Перенаправлення трафіку через фальшивий об'єкт або комп'ютер порушника.
джерело загрози	внутрішнє.
вразливість, що використовується при реалізації	Недостатній рівень надійності автентифікації повідомлень.
програми, які можуть застосовуватися при реалізації атаки	Програми перехоплення пакетів («сніфери»)
об’єкт атаки	Хост (вузол) мережі.
типові заходи захисту	Шифрування каналу передачі даних (SSL / TLS, SSH, HTTPS і ін.), Використанння програмних засобів для виявлення атак типу IP-спуффінг

Висновки до розділу 1

Проблеми низької безпеки вимагають нового способу розуміння технологічного та соціального впливу регіону, і, отже, майбутні політичні проблеми можуть бути вирішені лише після того, як природа кризи виникне. У курсі розглядається література про злочинність, відповідаючи на питання

дослідження та її здатність дати уявлення про природу регіональної безпеки. Низький рівень безпеки – це область, яка недостатньо зрозуміла.

З цієї причини важливо зосередитися на ідеях, які важливі для обговорення співпраці, безпеки та управління. Небезпека вважається політичною, економічною та соціальною проблемою, яка постійно розвивається у всьому світі. Розуміння безпеки, яке швидко змінилося протягом минулого століття, вплинуло на безпеку на основі оцінки ризиків. Ця стаття зосереджується на Європі та Україні, які визначаються їх географічним, культурним чи історичним контекстом. Краще розуміння європейської безпеки та прямих наслідків війн і конфліктів минулого століття.

Протягом останніх років війни та конфлікти змінили ситуацію з безпекою за межами військової системи, і розширена безпека еволюціонувала від суто самооборони до більш широкої ідеології, включаючи невійськову безпеку. Однак тероризм не є дійсним поняттям, і це визначення не може бути узгоджено з однією з цих цілей. Натомість важливо поєднувати загрозу і безпеку з місцем і часом, оскільки ці дві ідеї різні для людей, часів, часів і часів.

РОЗДІЛ 2
МЕТОДИ ЗАХИСТУ КОРПОРАТИВНОЇ ПОШТИ ВІД КІБЕРАТАК ЗА ДОПОМОГОЮ СКАНЕРІВ ПОШТИ

2.1.Вдосконалення методів захисту корпоративної пошти від кібератак за допомогою сканерів пошти

Сканери безпеки — це програмне забезпечення або інструменти, що використовуються для вимірювання та моніторингу мереж і комп'ютерів, які допомагають сканувати мережі, комп'ютери та програми для виявлення проблем безпеки, а також діагностики та усунення вразливостей. Сканер вразливостей дозволяє відстежувати різні програми в системі «дір», якими можуть скористатися зловмисники.

Основне призначення мережевого сканера — знайомство з відвідувачами, створення топології мережі, пізнання відкритих портів і служб, які їх обслуговують, а також операційної системи [12, с.89-96].

Сканування портів TCP за допомогою протоколу модифікації ідентифікації Протокол ідентифікує вас за іменем (ім'ям користувача або паролем, вказаними під час входу) власника будь-якого шляху, що виконується на пов'язаному сервері, навіть якщо сам шлях не починається.

Хост відправляє на певний порт сервера SYN-пакет, як би маючи намір створити з'єднання, і очікує відповідь client -> SYN server -> SYN|ACK client -> RST ---------- client -> SYN server -> RST|ACK.

Переваги:

- деякі сервери здатні зареєструвати такого роду сканування.

Недоліки:

- необхідні права адміністратора (root).

ACK Scan Цей розширений метод зазвичай використовується для відкриття набору правил брандмауера. Зокрема, це допомагає визначити, чи є статус

брандмауера простим фільтром пакетів, який блокує брандмауери чи вхідні пакети SYN. Цей тип сканування надсилає пакет ACK (з випадковим чином видимим підтвердженням/порядковими номерами) на вказані порти. Якщо повертається RST, порти класифікуються як закриті («нефільтровані») безпосередньо на хості.

Якщо нічого не повернуто (або якщо повідомлення ICMP не «повернено»), порт встановлюється на «фільтр», тобто блокувати фільтр або брандмауер. Очевидно, сканування вказує на відкриті порти. Сканування разом ping - комбінації Визначення стану сервера методом ICMP-сканування [14, с.87-91].

Хост пересилає сервера ICMP-повідомлення і чекає отримання відповіді - ICMP-повідомлення. • Якщо прийом відповіді успішний, значить маршрутизація виконана, сервер працездатний і швидше за все чекає запит на з'єднання. • Щоб здійснити запиту застосовується програма ping.

Nmap ("Network Mapper") – це утиліта з відкритим вихідним кодом для дослідження мережі та перевірки безпеки мереж та виявлення активних мережевих сервісів. Він був розроблений для швидкого сканування великих мереж, але відмінно працює на окремих хостах. Nmap працює на всіх основних комп'ютерних операційних системах, а офіційні виконавчі пакети доступні для Linux, Windows і Mac OS X [13, с.218-227].

На додаток до виконуваного файлу класичного командного рядка Nmap, є утиліта графічного інтерфейсу користувача (Zenmap), гнучкий інструмент для відправки, перенаправлення та відновлення (Ncat), утиліта для порівняння результатів сканування (Ndiff) і створення пакетів і аналіз відповідей. інструмент (Nping).). Nmap використовує багато різних методів сканування, таких як UDP, TCP (увімкнути), TCP SYN, FTP-проксі, зворотний ідентифікатор, ICMP (ping), FIN, ACK, Xmas дерево, SYN- та NULL сканування.

Nmap також підтримує ряд додаткових функцій, а саме: систему дистанційного зондування віддаленої системи, невидиме сканування, затримку та реверсування пакетів, паралельне сканування, гостьову маршрутизацію за допомогою роздільника та селектора ping, сканування бази даних фільтрів, пряме

(без використання portmapper) RPC-сканування, сканування з використанням IP-43 фрагментації, швидкий пошук вразливостей SQL Injection, а також довільне вказування IP-адрес та номерів портів мереж, що скануються [15, с.105-109].

Коли Nmap запущено, ви можете отримати наступні інструкції на екрані без будь-яких опцій: Програма: можна використовувати nmap (тип сканування). Приклад: scanme.Nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254 -iL: використовувати список хостів/мереж із файлу; -iR: вибрати довільні цілі РОЗРОБКА HOOST: -sL: Сканувати до списку - створити список цілей для простого сканування -sP: Пінг сканування - просто визначити, чи працює хост -PN: Розцінювати все хости як працюючі - пропустити виявлення хостів -PS/PA/PU [список_портів]: TCP SYN/ACK чи UDP пінгування заданих хостів -PE/PP/PM [16, с.323-324].

Пінгування з використанням ICMP exo запитів, запитів тимчасової мітки і мережевої маски -PO [список_протоколів]: Пінгування з використанням IP протоколу -n/-R: Никогда не производить DNS разрешение/Всегда производить разрешение РІЗНІ ПРИЙОМИ СКАНУВАННЯ: -sS/sT/sA/sW/sM: SYN/з використанням системного виклику Connect()/ACK/ Window/Maimon сканування -sU: UDP сканування -sN/sF/sX: TCP Null, FIN и Xmas сканування --scanflags : Задати власні TCP флаги -sI : "Лініве" (Idle) сканування -sO: Сканування IP протоколу -b : FTP bounce сканування ВИЗНАЧЕННЯ ПОРТІВ І ПОРЯДКУ СКАНУВАННЯ: -p : Сканування тільки певних портів Приклад: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080 -F: Швидке сканування Сканування обмеженої кількості портів -r: Сканувати порти послідовно - не використовувати випадковий порядок портів ВИЗНАЧЕННЯ ОС: -O: Активувати функцію визначення ОС [14, с.87-91].

Аналізатор трафіку або аналізатор – це програма або мікропрограмне забезпечення, призначене для захоплення та подальшого аналізу або просто аналізу мережевого трафіку для інших вузлів.

Перехоплення трафіку може здійснюватися:

• звичайним «прослуховуванням» мережевого інтерфейсу (метод ефективний при використанні в сегменті концентраторів (хабів) замість комутаторів (світчей), інакше метод малоефективний, оскільки на сніфер потрапляють лише окремі фрейми);

• підключенням сніфера в розрив каналу;

• відгалуженням (програмним або апаратним) трафіку і спрямуванням його копії на сніфер;

• через аналіз побічних електромагнітних випромінювань і відновлення трафіку, що таким чином прослуховується;

• через атаку на канальному (MAC-spoofing) або мережевому рівні (IPspoofing), що приводить до перенаправлення трафіку жертви або всього трафіку сегменту на сніфер з подальшим поверненням трафіку в належну адресу.

Аналіз трафіку, що пройшов через сніфер, дозволяє:

• Виявити паразитний, вірусний і закільцований трафік, наявність якого збільшує завантаження мережного устаткування і каналів зв'язку (сніфери тут малоефективні; як правило, для цих цілей використовують збір різноманітної статистики серверами і активним мережним устаткуванням і її подальший аналіз).

• Виявити в мережі шкідливе і несанкціоноване ПЗ, наприклад, мережеві сканери, флудери, троянські програми, клієнти пірінгових мереж та інші (це зазвичай роблять за допомогою спеціалізованих сніферів — моніторів мережної активності).

• Перехопити будь-який незашифрований (а деколи і зашифрований) призначений для користувача трафік з метою отримання паролів і іншої інформації.

• Локалізувати несправність мережі або помилку конфігурації мережних агентів (для цієї мети сніфери часто застосовуються системними адміністраторами) [17, с.136-143].

Tcpdump (від TCP і англ. dump — звалище, скидати) — сніфер, утиліта UNIX, що дозволяє захоплювати і аналізувати мережний трафік, що проходить через комп'ютер, на якому запущена ця програма. Основні призначення tcpdump:

• Налагодження мережевих програм

• Налагодження мережі і мережної конфігурації в цілому

• Програмна реалізація Програма складається з двох основних частин: частини захоплення пакетів (звернення до бібліотеки, libcap (Linux) або pcap (Windows)) і частини відображення захоплених пакетів (яка на рівні вихідного коду є модульною і для підтримки нового протоколу досить додати новий модуль) [18, с.179-281].

Розділ видалення пакетів (на початку) проходить «форму вибору пакетів» (після всіх описових рядків) у бібліотеці захоплення пакетів, збирає вираз виразу (у форматі префікса) і передає його у виділений рядок. Зовнішній вигляд також відповідає вимогам формули в передньому примірнику.

Розділ парку показує і вибирає парки, які були зняті в передньому бампері, і випускає їх, як правило, в громадській думці, відповідно до певної категорії. Якщо деталі пакета чітко визначені, програма перевіряє для кожного мережевого пакета, чи є в ньому модуль дешифрування і, якщо так, відповідний (і порівнянний) тип стандартних та інших інструментів у протоколі.

Синтаксис: Tcpdump [-aAdDeflLnNOpqRStuUvxX] [-c count] [-C file_size] [-E algo:secret] [-F file] [-i interface] [-M secret] [-r file] [-s snaplen] [-T type] [-w file] [-W filecount] [-y datalinktype] [-Z user] [expression] Найбільш популярні ключі:

• c count вийти після отримання певної кількості пакетів.

• F File використовувати file для введення фільтруючого вираження. Вираз, вказаний в командному рядку, буде ігноруватися.

• i interface збирати пакети тільки на певному інтерфейсі. Якщо не вказано - береться мінімальний за номером інтерфейс (виключаючи loopback).

Для Linux-ядер 2.2 і новіших, можливо вказати 'any', тоді буде відбуватися збір на всіх інтерфейсах, але вони не будуть переведені в режим promiscuous [19, с.68-76].

• n не перетворювати адресу хосту в ім'я. Може бути використано, якщо необхідно уникати DNS-запитів.

• nn не перетворювати протокол і номер порту в їх імена.

• N не виводити доменну частину імені хоста.

Наприклад, при цьому ключі буде виводиться "nic" замість "nic.ddn.mil" • p не переводити інтерфейс в режим promiscuous. Слід зауважити, що інтерфейс може бути в режимі promiscuous з інших причин. • r file читати пакети з file (який, був створений з ключем -w).

Якщо file вказаний як "-", то використовується стандартне введення. • t не виводити тимчасової штамп (timestamp) в кожному рядку дампа (dump). • tt висновок не форматований тимчасової штамп в кожному рядку дампа. • ttt виводити різницю (в мікросекундах) між поточною і попередньої рядками дампа. • tttt виводити тимчасової штамп разом з датою в форматі за замовчуванням в кожному рядку дампа. • v докладний висновок. Для ще більш докладного виведення використовуються: -vv і -vvv. • w file писати "сирі" пакети в file перед тим як зробити їх розбір і вивести. Вони можуть бути пізніше виведені з ключем -r.

Якщо файл відображається як «-», використовується стандартний вихід. • x Надрукуйте кожен пакет (без заголовків рівня підключення) у шістнадцятковому форматі. • На додаток до шістнадцяткового представлення для виведення значень ASCII, X. Wireshark (раніше Ethereal) — це програма для аналізу мережевих пакетів Ethernet та інших мереж (снайперів) із безкоштовним вихідним кодом. Має графічний інтерфейс користувача.

У червні 2006 року проект був перейменований на Wireshark через проблеми з торговою маркою. Програмна реалізація. Функціональність, яку надає Wireshark, дуже схожа з можливостями програми tcpdump, проте Wireshark має графічний інтерфейс користувача і значно більше можливостей із сортування і фільтрації інформації. Програма дозволяє користувачеві переглядати весь трафік, що проходить по мережі, в режимі реального часу, переводячи мережну карту в promiscuous mode режим [20, с.24-28].

Wireshark – це програма, яка розпізнає природу різних протоколів протоколів і, таким чином, допомагає вам проаналізувати взаємозв’язок, демонструючи значення кожного поля протоколу на будь-якому рівні. Оскільки

використовується для захоплення пакетів, можна отримати інформацію лише про мережі, які підтримує ця бібліотека. Але, Wireshark вміє працювати з безліччю форматів початкових даних, відповідно, можна відкривати файли даних, захоплених іншими програмами, що розширює можливості захоплення.

Програма розповсюджується під вільною ліцензією GNU GPL і використовує для формування графічного інтерфейсу кросплатформову бібліотеку GTK+. Існують версії для більшості типів UNIX, зокрема GNU/Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, а також для Microsoft Windows. Wireshark містить два види фільтрів - захоплення (Capture Filters) і відображення (Display Filters). Capture Filters. Вони служать для фільтрації ще на етапі захоплення трафіку.

Але поки, звичайно, ви можете втратити частину цього. Фільтр - це набір значень, які можна комбінувати з логічними функціями (і, або, ні), якщо це необхідно. Щоб скористатися ним, потрібно зайти в меню Capture, потім Options, і в поле Capture Filter набрати, наприклад, host 8.8.8.8 (або, наприклад, net 192.168.0.0./24). Так само, звичайно, можна вибрати і заздалегідь створений фільтр (за це відповідає кнопка Capture Filter) [21, с.20-24].

У будь-якому з варіантів фільтр з'явиться біля інтерфейсу, можна жати Start. Display Filters. Вони фільтрують лише транспортні засоби, які вже вважаються стандартними, наприклад, протокол, адреса, конкретні поля в протоколі. Особливу увагу слід звернути на функцію синтаксичного аналізу, яка забезпечує три елементи взаємодії: • прямий виклик (виклик парсера); • виклик (парсер визначає значення ключового поля, отримане при порівнянні низькорівневого протоколу; наприклад, значення поля «порт» у заголовку пакету TCP); • статевий акт (викликаний разбірник визначається шляхом пошуку патернів в уже згадуваному буфері); Wireshark надає можливість для підключення додаткових (в тому числі самостійно розроблених) модулів розбору трафіку.

Для об'єднання декількох виразів можна застосовувати:

• && - обидва вирази повинні бути вірними для пакета;

• || - може бути вірним один з виразів.

Основні переваги та недоліки. Основні переваги інструменту:

• Підтримка великої кількості мережевих протоколів (в тому числі протоколів IP-телефонії);

• Підтримка різних форматів мережевих трас;

• Можливість розширення (можливість створення і підключення додаткових модулів розбору);

• Детальна система фільтрації мережевих пакетів;

• Можливість відновлення потоків TCP; Недоліки:

• Відновлений потік не розглядається інструментом як єдиний буфер пам'яті, внаслідок чого його подальша обробка неможлива;

• Код модулів розбору містить функції, що відповідають за візуалізацію результатів (логіка розбору перемішується з логікою відображення в графічному інтерфейсі);

• Відсутня можливість виконання деякого дії в разі виявлення сигнатур в трафіку [22, с.193-199].

2.2. Вдосконалення методів захисту корпоративної пошти від кібератак за допомогою сканерів пошти

Система моніторингу мережі - це система, яка постійно контролює комп'ютерну мережу в пошуках повільних або незручних систем і повідомляє адміністратора про збій за допомогою сповіщення. Ці функції є частиною функції управління мережею. Наприклад, щоб визначити структуру сайту, система відстеження може надіслати HTTP-запит на отримання сторінки; ви можете надсилати тестові повідомлення на сервер по SMTP і отримати по IMAP або POP3 [23, с.62-64].

Невдалі запити (наприклад, коли не вдається встановити з'єднання, закінчується після запланованого часу або коли повідомлення не доставлено) зазвичай викликають реакцію системи. Як люди можуть поводитися:

• Скарги, надіслані системним адміністратором.

• Система захищає систему від тимчасового вимкнення сервера, доки проблему не буде вирішено.

Для того щоб підтримувати графік роботи, потрібно регулярно контролювати локальну мережу, яка є основою всієї мережі. Лідерство - це перший крок в управлінні мережею. Через важливість цієї функції її часто відрізняють від інших функцій системи управління та реалізують спеціальними засобами.

Такий поділ функцій контролю та управління важливий для малих і середніх мереж, оскільки створення інтегрованого управління економічно недоцільно. Використовуючи незалежний метод моніторингу, який допомагає веб-майстру виявляти проблеми з мережевими інструментами, а також зупиняти чи переглядати їх, він може зробити це вручну [24, с.295-307].

Процес моніторингу мережі зазвичай поділяється на два етапи:

• моніторинг.

• аналіз.

На етапі моніторингу виконується більш проста процедура - процедура збору первинних даних про роботу мережі: статистики про кількість циркулюючих в мережі кадрів і пакетів різних протоколів, стан портів концентраторів, комутаторів і маршрутизаторів та іншого проміжного обладнання.

Тепер, коли фаза аналізу на місці, це складний і логічний спосіб зрозуміти інформацію, зібрану в контексті моніторингу, порівняти її з інформацією, наданою раніше, і передбачити можливі причини затримки або ненадійної роботи. Завдання моніторингу вирішують програмні та приладові лічильники, сканери, мережеві аналітики, вбудовані у вигляді пристроїв керування комунікаційним обладнанням, а також персонал системи контролю.

Аналітична робота вимагає великої участі людини та використання складних інструментів, таких як експертна система, яка збирає практичний досвід багатьох співробітників. Усі канали моніторингу та аналізу мережі можна розділити на кілька основних категорій:

• Система управління мережею - система, яка поєднує збір даних з конфігурацією вузлів і мережевим комунікаційним обладнанням, а також інформацією про трафік.

Ці системи не тільки відстежують та аналізують, але й працюють в автоматизованій або автоматизованій частині управління мережею – вмикаючи та вимикаючи порти пристроїв, змінюючи показники хоста для адрес адресного рядка, комутаторів і маршрутизаторів тощо.

Прикладами систем управління можуть служити популярні системи HPOpenView, SunNetManager, IBMNetView. • Управління системою. Система управління часто виконує функції, подібні до системи керування, але в порівнянні з іншими речами. У першому випадку об'єктом управління є програмне забезпечення та мережеве комп'ютерне обладнання, а в другому - пристрій зв'язку [25, с.5-12].

Однак деякі функції цих двох типів систем керування можна дублювати, наприклад, системи керування можуть виконувати простий аналіз мережевого трафіку. Найпопулярніші системи керування системою включають LANDesk, IBM Tivoli, Microsoft Systems Management Server, HP OpenView, Novell ZENworks та CA Unicenter. • Вбудовані системи.

Ці системи реалізовані у програмному забезпеченні та архівних матеріалах, встановлених у пристроях зв’язку, а також у вигляді програмного забезпечення, вбудованого в операційну систему. Вони виконують функцію перевірки і управління тільки одним приладом, і це основна відмінність системи управління [26, с.126-128].

Прикладом засобів цього класу може служити модуль управління концентратором Distrebuted 5000, реалізує функції автосигментації портів при виявленні несправностей, розміщення портів перед хабом та інші. Зазвичай він має вбудовані модулі, які також діють як SNMP, які надають інструменти конфігурації обладнання для керування системою. • аналітики протоколів (Protocol analyzers).

Являють собою програмну або апаратно-програмну систему, на відміну від системи управління, яка обмежується функцією моніторингу та аналізу транспортних засобів у мережі. Правильний аналіз протоколів може охопити та проаналізувати велику кількість протоколів, що використовуються в мережі – зазвичай десятки. Аналітики протоколів дозволяють налаштувати деякі логічні речі для окремого пакування та повного декодування захоплених пакетів, тобто продемонструвати між користувачами вміст протоколів пакетів різних рівнів в одній категорії та витягти вміст кожного поле. кожен парк.

Інструменти тестування та перевірки для подвійної системи. Зазвичай ці пристрої можна розділити на чотири основні групи: моніторинг мережі, обладнання для перевірки кабельної системи, кабельний сканер і мультиметр. Мережні монітори (також звані аналітичними мережами) призначені для перевірки проводів різних фаз. Слід розрізняти моніторинг мережі та аналітику протоколів. Мережні трекери збирають дані тільки про номери доріг - середню вагу всієї мережі, середню потужність парку і тип помилки і т.п.

Метою наступних інструментів системи аутентифікації є їх ідентифікація. Рішення приймається відповідно до вимог цієї ж міжнародної системи. Для вимірювання мідної системи використовуються кабельні сканери. Плануються випробування, щоб перевірити, чи не обірвався дріт. Експертна система. Цей тип системи збирає людські знання для виявлення причин заторів і можливих шляхів реалізації мережі [27, с.144-147].

Експертні системи часто реалізуються різними способами моніторингу та аналізу мереж: системи управління мережами, аналітики протоколів, мережеві аналітики. Найпростішим варіантом експертної системи є системна система. Розширені системи — це те, що ми називаємо базовими знаннями з інтелектуальними функціями.

Прикладом системи є спеціалізована система, вбудована в Cabletron Spectrum Management System. • Багато інструментів для аналізу та оцінки. Поряд із поширенням мереж загального користування виникає потреба в розробці доступних мобільних пристроїв, які інтегрують функціональність багатьох

пристроїв: аналізатори протоколів, сканери кабелю та деякі інші види програмного забезпечення для управління мережею [28, с.65-68].

Прикладом такого типу інструменту є Compas MicrotestInc. або LANMeter компанії FlukeCorp. Дивіться відповідь на один із інструментів керування системою, а саме на Zabbix Zabbix та рішення для розповсюдження компаній, що базуються на контролі, з відкритим кодом; програмне забезпечення орієнтоване на відстеження кількох мережевих стандартів, сервер працює добре. Zabbix використовує просту систему сповіщень, яка дозволяє користувачам встановлювати повідомлення електронною поштою для всього.

Ця функція дозволяє швидко реагувати на проблеми сервера. Zabbix пропонує чудові можливості звітності та візуалізації даних на основі історичних даних. Zabbix — це високоінтегроване рішення для моніторингу мережі, яке пропонує багато функцій в одному пакеті: збір даних: • доступ і тестування продуктивності • підтримка SNMP (контроль і запит), моніторинг IPMI, JMX, VMware • митні перевірки • збір необхідних даних через певні проміжки часу • сервер або проксі та агенти Гнучкі пороги: • Ви можете визначити дуже гнучкі обмеження проблем, які називаються тригерами, які посилаються на значення в базі даних сервера.

Налаштовуються оповіщення: • відправка повідомлень може бути налаштована відповідно до розкладу ескалації, одержувачем, типом носія • повідомлення можуть бути стислими та інформативними • автоматичні дії включають віддалені команди.

Графіки у реальному часі: • відслідковують елементи негайно відображаються за допомогою вбудованої функції побудови графіків Можливості веб-моніторингу: • Zabbix може слідувати шляху імітації миші на веб-сайті і перевіряти функціональність і час відгуку [29, с.234-235].

Можливість надати розширені знання: • Можливість створити власний дизайн, який може поєднувати багато речей в один спосіб • Картка взаємодії • Екран і слайд-шоу, як переглянути • Звіт • Тип контрольованих інструментів

верхнього рівня (бізнес) Зберігати історію : • інформація, що зберігається в архіві • історія, створена • вбудована під час демонтажних робіт.

Просте налаштування • додати відслідковують пристрою в якості хостів • хости підібрані для моніторингу, один раз в базі • застосовувати шаблони для відслідковується пристроїв Використання шаблонів: • угруповання перевірок в шаблонах • шаблони можуть наслідувати інші шаблони 55 • виявлення мережі • автоматичне виявлення мережевих пристроїв • автоматична реєстрація агента • виявлення файлових систем, мережевих інтерфейсів і ідентифікаторів SNMP

Веб-посилання: • Веб-видимість у PHP • Доступний з будь-якого місця • Ви можете пройти через Zabbix API: Система ліцензування: • Аутентифікація користувачів • Деякі користувачі можуть бути розділені на декілька ідей, повних, легких і легко розширених: для моніторингу • може бути розгорнутий як на Linux, так і на Windows Двійкові демони: • написано на C, для продуктивності і невеликого обсягу пам'яті • легко переноситься Готовий для використання у складному середовищі: • віддалений моніторинг став простіше завдяки використанню Zabbix проксі Zabbix підтримує як опитування, так і захоплення [30, с.125-130].

Усі звіти та статистичні дані, а також параметри налаштування доступні через веб-інтерфейс. Веб-інтерфейс дозволяє оцінювати стан мережі та статус сервера з будь-якого місця. При належному налаштуванні Zabbix може відігравати важливу роль у моніторингу вашої IT-інфраструктури. Це однаково стосується невеликих організацій із кількома серверами та великих компаній із кількома серверами. Zabbix безкоштовний. Zabbix надає комерційну підтримку. Загальна публічна ліцензія GPL.

Це означає, що його походження надається безкоштовно і доступне широкому загалу. Багато глобальних корпорацій покладаються на Zabbix як на центральний контрольний сайт.

Здебільшого це заява влади; • Можна використовувати такі бази даних, як SQLite, MySQL та Oracle; • Зовнішній вигляд сайту відповідає за моніторинг та управління діяльністю, а також перегляд. Веб-сайт системи написаний на PHP; •

Співробітник Zabbix, який працює над пристроєм (пристроями), який хоче отримати інформацію. Обов’язково, але якщо його неможливо встановити на пристроях, це можна зробити за допомогою SNMP (простого протоколу керування мережею) [31, с.164-166].

Поглиблений контроль (DPP) — це поширена назва технології, яка допомагає вам збирати, аналізувати, сортувати, контролювати та редагувати веб-сторінки відповідно до вмісту в реальному часі. Іноді використовується коротке слово - DPP (Deep Packet Processing), який має на увазі такі дії над пакетами, як модифікація, фільтрація або перенаправлення.

Сьогодні обидва терміни - DPI і DPP - часто використовуються як взаємозамінні. Модель розвитку DPI Технології інспекції трафіку розвивалися послідовно, кожна наступна успадковувала частина попередніх механізмів і додавала свої:

1) Shallow Packet Inspection,

2) Medium Packet Inspection,

3) Deep Packet Inspection. Shallow Packet Inspection (Слабкий аналіз пакетів) - технологія аналізу трафіку, яка ґрунтується виключно на заголовках пакету (не аналізує вміст корисного навантаження пакета). Це перша реалізація технології інспектування трафіку. Менш вимоглива до ресурсів, ніж MPI і DPI, за рахунок чого, може обробляти набагато більші обсяги трафіку з високою точність визначення [32].

Технологія широко використовується в багатьох системних брандмауерах, маршрутизаторах (ACL) та багатьох інших. Однак назву технології не слід плутати з технологією вимірювання структури пачки – технологією перевірки, чи добре йде рух. У середині пакетного сканування знаходиться технологія аналізу програмного забезпечення на базі автомобілів, яка була запущена, але має плату безпеки та комунікацій проксі.

Як правило, назва технології MPI заміщається позначенням «application proxy». Частково аналізує вміст пакетів по визначеним правилам. Не використовуються складні методи аналізу (сигнатурний і т.д.). Так само є однією

з форм брандмауера. Технологія Deep Packet Inspection (Глибокий аналіз пакетів) виникла через необхідність аналізувати, контролювати і управляти переданим трафіком.

Технологія DPI розвивалися в основному за рахунок швидкого зростання потужності мікросхем (процесорів), їх продуктивності. Нащадок системи DPI. Деякі джерела містять інформацію про систему управління трафіком DPI. Існують два покоління інструментів: Перше покоління: модифіковано для вирішення короткострокових проблем і має метод аналізу сигнатур. Друге покоління: багато аналітичних і вимірювальних інструментів, а також евристичних методів і поведінки, включаючи інструменти для рейтингування та управління політикою [33].

Іноді в залежності від продуктивності пристрої поділяються на ланки: перше покоління до 10 Гбіт/с, друге від 10 до 100 і третє покоління вище 100. Технологія DPI використовується з такими сучасними рішеннями - Системи операційної та технічної підтримки (COPC), антивірусні рішення, системи керування трафіком, сучасні брандмауери.

Різниця між системою DPI і брандмауером полягає в наступному: • Система DPI не тільки аналізує заголовки пакетів, але й аналізує всі компоненти автомобіля на рівні моделі OSI від другого і вище. Система DPI може приймати рішення не тільки в двох пакетах, але і в прямих випадках, які зустрічаються в деяких протокольних програмах. Для цього можна використовувати статистичний аналіз (наприклад, статистичний аналіз частоти окремих об’єктів, довжини парку тощо). • Система DPI, на відміну від брандмауера, використовує різноманітні дорожні дії (сортування, зменшення інтернет-трафіку, визначення пріоритетів, маркування, зберігання тощо) [34].

Bypass - високопродуктивний комутатор, основне завдання якого пропускати трафік або безпосередньо (без обробки), або відправляти трафік на пристрій обробки і аналізу трафіку - Front-End, Bypass постійно стежить за зв'язком з Front-End компонентом і в випадках втрати зв'язку або отримання повідомлень від Front-End, про труднощі обробки трафіку, починає пропускати

трафік безпосередньо до прикордонного маршрутизатора. Існують різні типи 59 Bypass інтерфейсів: мідні (не більше 1 Гбіт / с) і оптичні (від 1 до 100 Гбіт / с). Підтримується оптичне віддзеркалення трафіку «як є» і відповідно можливий збір статистики або підключення СОРЗ. Front-End - могз DPI системи - центр обробки інформації відповідно до налаштованих / наявних політик. По суті це модульний центр обробки інформації.

Back-End - це високопродуктивний кеш-сервер для оперативного використання баз сигнатур, різної статистики, політик і різних правил перенаправлення трафіку. Основним завданням Back-End є моментальне надання інформації для Front-End компоненти. Як правило, кеш-сервера мають високу степ резервування своїх компонентів, підтримують гарячу заміну і вміють балансувати навантаження (для роботи в кластері). PCRF-сервер (Policy and charging rules function) - один з основних компонентів DPI систем - сервер визначення правил і політик. Основна роль при отриманні від Front-End`а ідентифікатора користувача / абонента, повідомити Front-End`у відповідний номер політики.

Далі Front-End запитує подробиці відповідної політики на Back-End'і. У деяких DPI системах роль PCRF компонента або частину функцій виконує Subscriber Manager сервер. Disk array Server - Сервер дисковий масив призначений для зберігання великих обсягів інформації (статистики, різних баз даних, іноді копій трафіку). Як правило, взаємодіє тільки з Back-End`дом для актуалізації кеш-фонду останнього. NMS Server (Network Management Server) - Сервер управління системою [35].

Update Server - Сервер оновлення. Основне завдання отримувати оновлення: системні оновлення, оновлення сигнатур і політик, моделей поведінки і т.д. з сервера поновлення виробника, через захищене з'єднання. Subscriber Manager - Сервер і / або програмний компонент системи є координаційним центром DPI систем управління трафіком, реалізує можливості персоналізації і диференціювання абонентських послуг (прив'язка до користувача / пристрою / мережі). VAS Server (Value Added Services Server) - Сервер додаткових сервісів.

Виробники DPI систем управління трафіком інтенсивно розвивають VAS сервіси, через те, що він надає доступ до сервісів, додаткових сервісів та додаткових сервісів для розробників/розробників, таким чином розширюючи систему. Система мережевого аналізу (NTA) призначена для координації інформації та виявлення ознак атак, часто спрямованих (APT).

З їх допомогою можна проводити ретроспективне вивчення мережевих подій, виявляти і розслідувати операції зловмисників в інформаційній інфраструктурі підприємства, а також ефективно реагувати на відповідні події. Такі системи відмінно доповнюють продукти класу Endpoint Detection and Response (EDR), можуть служити багатим джерелом 60 відомостей для SIEM-систем або центрів моніторингу та оперативного реагування на інциденти інформаційної безпеки [36, с.16-19].

Рішення на основі NTA відстежують трафік до та з загальнодоступних мереж і використовують різноманітні методи (аналіз поведінки, машинне навчання) для швидкого виявлення, аналізу та усунення загроз, які можуть залишатися прихованими. NO можна використовувати в лінії будь-якого розміру, а також у будь-якій будівлі: закритій, хмарній, змішаній. Інтеграція з EDR та SIEM призводить до непов’язаної інформації.

У такій схемі NTA це відповідальність онлайн-видання новин, EDR за надання наскрізної інформації та SIEM за збір інформації. Основними напрямками діяльності NTA є: • аналіз транспортних засобів як на стороні мережі, так і в інфраструктурі, • виявлення атак за допомогою технології виявлення, • допомога у проведенні розслідувань. Зазвичай стандартні репозиторії NTA включають: • мережевий датчик, який збирає трафік, • інтегрований сервер керування, • панель інструментів.

Деякі рішення NTA поєднують можливості пошуку проблем безпеки з автоматизованими завданнями з реагування на ризики і пом'якшенням наслідків інцидентів. Інструменти цього типу постійно шукають в мережі підозрілі або шкідливі дані. Якщо в результаті сканування вдалося щось виявити, то NTA діагностує проблему, щоб визначити, в чому саме полягає загроза безпеці.

Ґрунтуючись на цьому діагнозі, продукт розгортає автоматизовані завдання, щоб допомогти нейтралізувати проблему, одночасно оповіщаючи співробітників інформаційної безпеки про неї [37, с.112-115].

Висновки до розділу 2

Отже, половина усіх кібератак здійснюються через корпоративні повідомлення, оскільки вони є потужним інструментом для компаній. Перш за все, потрібно переконатися, що вхідні повідомлення співробітника не є спамом. Якщо більшість листів не фільтрується або не видаляється одночасно, вони негайно завершують усі серверні програми.

Він може надіслати вам бомбу Zip або файл-бомбу. Мета полягає в тому, щоб один із мільйонів файлів, прихованих у zip-архіві, надіслали до поштової служби. Якщо компанія, яка не використовує антивірус, включає кількість вкладень до сканера, zip-архів може видалити всі служби електронної пошти, заповнюючи мільйони копій загального дискового простору. В результаті компанія не може спілкуватися зі своїми клієнтами.

Часто зловмисники розсилають «фішингові» листи, замасковані, наприклад, службами адвокатської діяльності компанії. Подібні повідомлення містять посилання на фейкові сайти, майже дублікати, повні фактів. Основна мета пошуку – ввести пароль від компаній, які налаштували приховану сторінку. Зокрема, такий лист може заразити вірусну систему: людина завантажує пов’язаний із повідомленням файл або відкриває рядок, у якому запускається шкідливе програмне забезпечення.

Щоб запобігти подібним атакам, служба електронної пошти повинна бути встановлена в хмарі. Наприклад, хмара Microsoft Azure вже забезпечила базовий захист від спаму, захисту від риболовлі та багато іншого.

РОЗДІЛ 3
РОЗРОБКА МЕХАНІЗМІВ ЗАХИСТУ КОРПОРАТИВНОЇ ПОШТИ ВІД КІБЕРАТАК ЗА ДОПОМОГОЮ СКАНЕРІВ ПОШТИ

3.1. Механізми захисту корпоративної пошти від кібератак за допомогою сканерів пошти

Брандмауер – це частина програмного забезпечення та програмного забезпечення в комп'ютерній мережі, яка відстежує та фільтрує мережевий пакет, що відповідає місцевим законам. Основною функцією брандмауера є захист мережі або окремих її заголовків.

Брандмауери також часто називають фільтрами, оскільки їх основна функція полягає в запобіганні (фільтрації) пакетів, які не відповідають критеріям, визначеним у конфігурації. Типові особливості брандмауерів (далі - МЕ):

• фільтрація доступу до відомих небезпечних служб;

• запобігання одержанню конфіденційної інформації із захищеної мережі, а також імпорту неправдивої інформації в надійну систему за допомогою простих у використанні сервісів;

• контроль доступу до мережі;

• він може записувати всі форми доступу як зовнішнього, так і внутрішнього, що дозволяє контролювати використання Інтернету через окремі мережі;

• регламентування порядку доступу до мережі;

• повідомлення про підозрілу діяльність, спробах зондування або атаки на вузли мережі або сам екран.

Структурний аналіз допомагає контролювати структуру з'єднання та призупиняти парки, які не відповідають очікуванням. Для цього аналізується інформація про дорожній рух. На відміну від фільтрації пакетів, аудит стану відстежує історію кожного посилання за допомогою карти станів. Загальна

інформація доступу включає IP-адресу джерела, IP-адресу хоста та інформацію про з’єднання. Переваги брандмауера та аналізу поведінки:

• Дозволяють проходження пакетів тільки для встановлених з'єднань;

• Прозорі для клієнтів і серверів, так як не розривають TCP-з'єднання. Недоліки міжмережевих екранів з аналізом стану:

• Реально використовуються тільки в мережевій інфраструктурі TCP/IP.

Хоча слід зазначити, що брандмауер і аналіз конфігурації можуть бути реалізовані в інших визначеннях протоколів, а також у пакеті 65 у фільтрі. Проаналізуйте протокол на рівні запиту, порівняйте поведінку протоколу з деякими розширеними профілями та з’ясуйте відмінності в поведінці. Це змушує брандмауер дозволяти або забороняти доступ залежно від того, як працює система. Програми на рівні брандмауера доступні для багатьох протоколів, у тому числі HTTP, БД (SQL), поштові (SMTP, POP, IMAP), VoIP і XML [38, с.298-303].

Переваги: • Можливість аутентифікації користувача; • слабкі місця в атаках підробки; • може аналізувати не тільки мережеву адресу номера порту, але й всю мережу мережі; • ведення детальних журналів; Недоліки: • Аналіз кожного парку займає багато часу; • Змініть кількість програм, що використовуються з протоколом, і можуть не відразу підтримувати нові мережі та протоколи. Поєднуйте нижчий рівень керування з вищим рівнем роботи.

Вони мають проксі-агента, що діє як посередник між двома хостами, які хочуть взаємодіяти один з одним, і ніколи не допускає прямої взаємодії між ними. Результатом успішної спроби встановлення з'єднання є створення двох окремих з'єднань - одне між клієнтом і проксі-агентом, інше - між проксі-агентом і реальним сервером.

Переваги: • Проксі має можливість запитувати аутентифікацію користувача; • менш схильні до деструктивних атак; • максимальний шанс проаналізувати весь мережевий пакет, а не мережеву адресу та номер порту; • виготовляти деталі; Недоліки: • витрачають багато часу на аналіз кожної пачки; • Розробка невеликої кількості програм, що використовуються з протоколом, і вони не можуть негайно підтримувати нові мережі та протоколи.

Він використовується для зменшення навантаження на брандмауер і для виконання спеціальної фільтрації та реєстрації, що може бути важко виконати на брандмауері. Крім цих типів брандмауерів, розрізняють наступні: кінцеві точки VPN. Для шифрування певного трафіку між захищеними мережами. Дві найбільш часто використовувані архітектури VPN – це шлюз шлюзу та шлюз хоста [39].

Використання гібридного брандмауера. Багато брандмауерів поєднують в собі продуктивність різних типів брандмауерів. Наприклад, більшість проксі-програм реалізують централізований пакет. Додаткові можливості контролю потужності. Необхідність вирішувати вхідні з'єднання не тільки після віддаленого використання, а й контролювати параметри безпеки для користувачів комп'ютерів.

Уніфіковане управління загрозами Міжмережеві екрани для веб-додатків. Міжмережеві екрани для віртуальних інфраструктур Міжмережеві екрани для окремих хостів і домашніх мереж Слід зазначити, що міжмережеві екрани ефективні тільки для трафіку, який вони можуть аналізувати. Незалежно від обраної технології брандмауера, якщо він не може розуміти трафік, який проходить через нього, він не може змістовно дозволити або заборонити його. Багато мережевих протоколів використовують криптографію, щоб приховати вміст.

Прикладами протоколів є IPsec, TLS, SSH і SRTP (Real Traffic Safety). Брандмауер також не може прочитати приховану інформацію, наприклад, якщо повідомлення електронної пошти зберігається за допомогою протоколу S / MIME або OpenPGP. Іншим прикладом повернення є те, що більшість брандмауерів не чують вхідних та вихідних дзвінків, навіть якщо вони не збережені. Наприклад, трафік IPv6 можна підключити до IPv4 різними способами. Вміст може бути не відкритим, але якщо брандмауер не розуміє використовуваного методу тунелювання, трафік неможливо пояснити.

У кожному разі вони захопили його, незважаючи на перешкоди, які ми навряд чи можемо уявити». Політика брандмауера. Політика брандмауера описує, як брандмауер обробляє трафік на певну IP-адресу разом із адресою, протоколом,

програмою та типом вмісту (наприклад, вміст). Перш ніж сформулювати протипожежну політику, вам необхідно проаналізувати вплив і визначити тип транспортного засобу, який потрібен організаціям. Аналіз впливу має базуватися на оцінці ризику та оцінці ризику [40, с.34].

Існують наступні типи політик брандмауера: • політика на основі IP-адреси та протоколу (IP-адреса та інші функції IP, IPv6, протоколи TCP та UDP, протокол ICMP); • політика на основі додатків; • політики ідентифікації користувачів; • мережеві політики. Брандмауер має можливості NAT. ОТ

Маршрутизатор NAT розташований на межі двох частин адреси і змінює IP-адресу з одного регіону на інший, щоб парк працював безперебійно. Маршрутизатор NAT має 68 підключень до кількох адрес і не повинен надсилати неправильну інформацію з одного адресного рядка в інший (наприклад, через протокол). Фіксований формат – відображає IP-адресу, яка не записується в IP-адресу на основі кожного з них.

Це особливо важливо, коли до пристрою потрібно отримати доступ із-за межі мережі. Динамічний NAT – показує IP-адресу, яка не зареєстрована на адресу, записану з груп IP-адрес. Dynamic NAT також розміщує пряму картку між незареєстрованою та зареєстрованою адресами, але карта може відрізнятися залежно від зареєстрованої адреси, доступної в пулі під час спілкування.

Перевантажений NAT (NAPT, NAT Overload, PAT, маскарадінг) - форма динамічного NAT, який відображає кілька незареєстрованих адрес в єдиний зареєстрований IP-адреса, скориставшись різними портами. Відомий також як PAT (Port Address Translation). При перевантаженні кожен комп'ютер в приватній мережі транслюється в ту же саму адресу, але з різним номером порту.

Топологічна мережа під час використання брандмауера Оскільки перша функція брандмауера полягає в запобіганні вхідних та вихідних (а іноді вихідних) брандмауерів, брандмауер повинен знаходитися в точці, де він входить у логічну межу. Зазвичай це означає, що брандмауер є вузлом, де потік використовується кількома потоками або об’єднаний в один потік.

3.2. Механізми захисту корпоративної пошти від кібератак за допомогою сканерів пошти

У цьому розділі ми повернемося до розділу безпеки від DDO і розглянемо, як захистити VPS і Fail2ban. Його основна мета — захистити неавторизованого одержувача, можливо, шляхом моніторингу складності великих портів і читання дерев (файлів входу).

Програма особливо ефективна проти так званих атак грубої сили, оскільки нейтралізує зловмисника від усіх пакетів, надісланих з пристрою, IP-адреса якого з тих чи інших причин внесена до чорного списку. Блокування налаштовується шляхом внесення змін до правил iptables. Отже, приступаємо до налаштування орендованого VPS-сервера. Щоб встановити Fail2ban, виконайте такі команди:

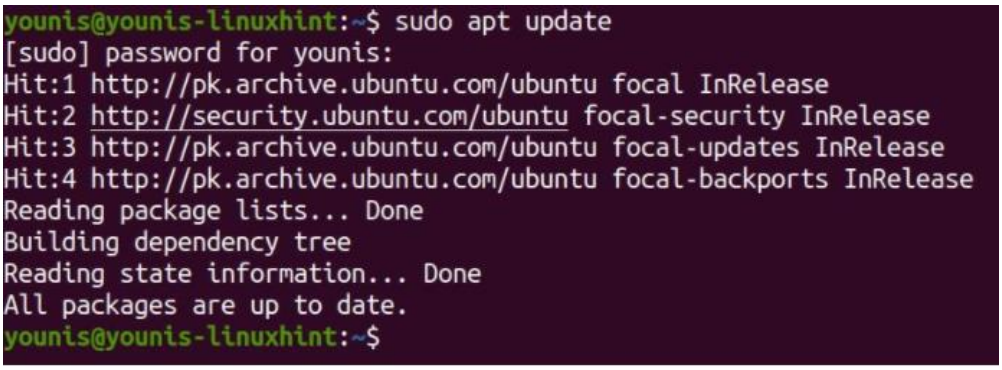

Рисунок 3.1 - Встановлення програмного забезпечення Fail2ban на Ubuntu 20.04 сервер

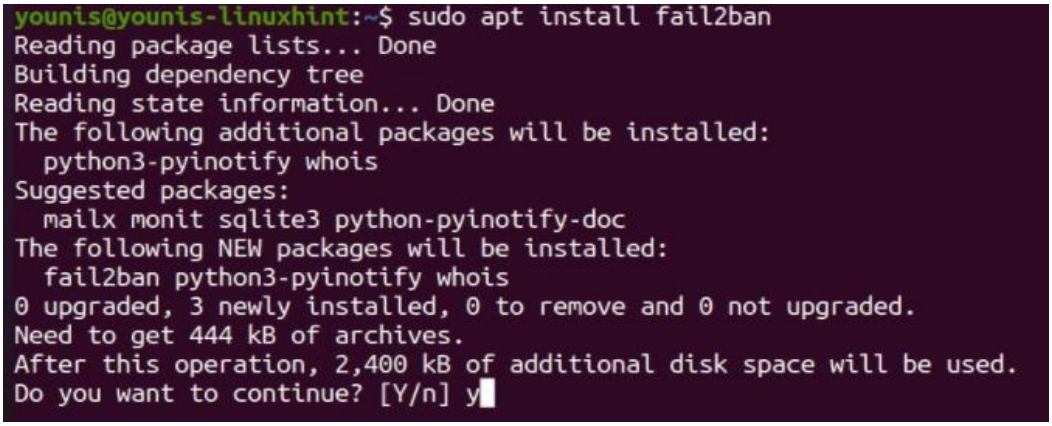

Рисунок 3.2 - Встановлення програмного забезпечення Fail2ban на Ubuntu 20.04 сервер.

Вам потрібно змінити файли конфігурації встановленого програмного забезпечення, щоб він працював належним чином. За замовчуванням є /etc/fail2ban/jail.conf. Однак розробники рекомендують утримуватися від зміни сервера, щоб уникнути проблем. Тому ми зробили копію цього файлу за допомогою команди:

Далі нам потрібно буде виконувати редагування тільки /etc/fail2ban/jail.local. Він буде підключений системою автоматично і має вищий пріоритет при виконанні. Відкриємо файл jail.local для редагування однієї з команд: sudo nano /etc/fail2ban/jail.local Звернімо увагу на секцію [DEFAULT]. Вона містить в собі основні правила, задані за замовчуванням для Fail2ban [37, с.112-115].

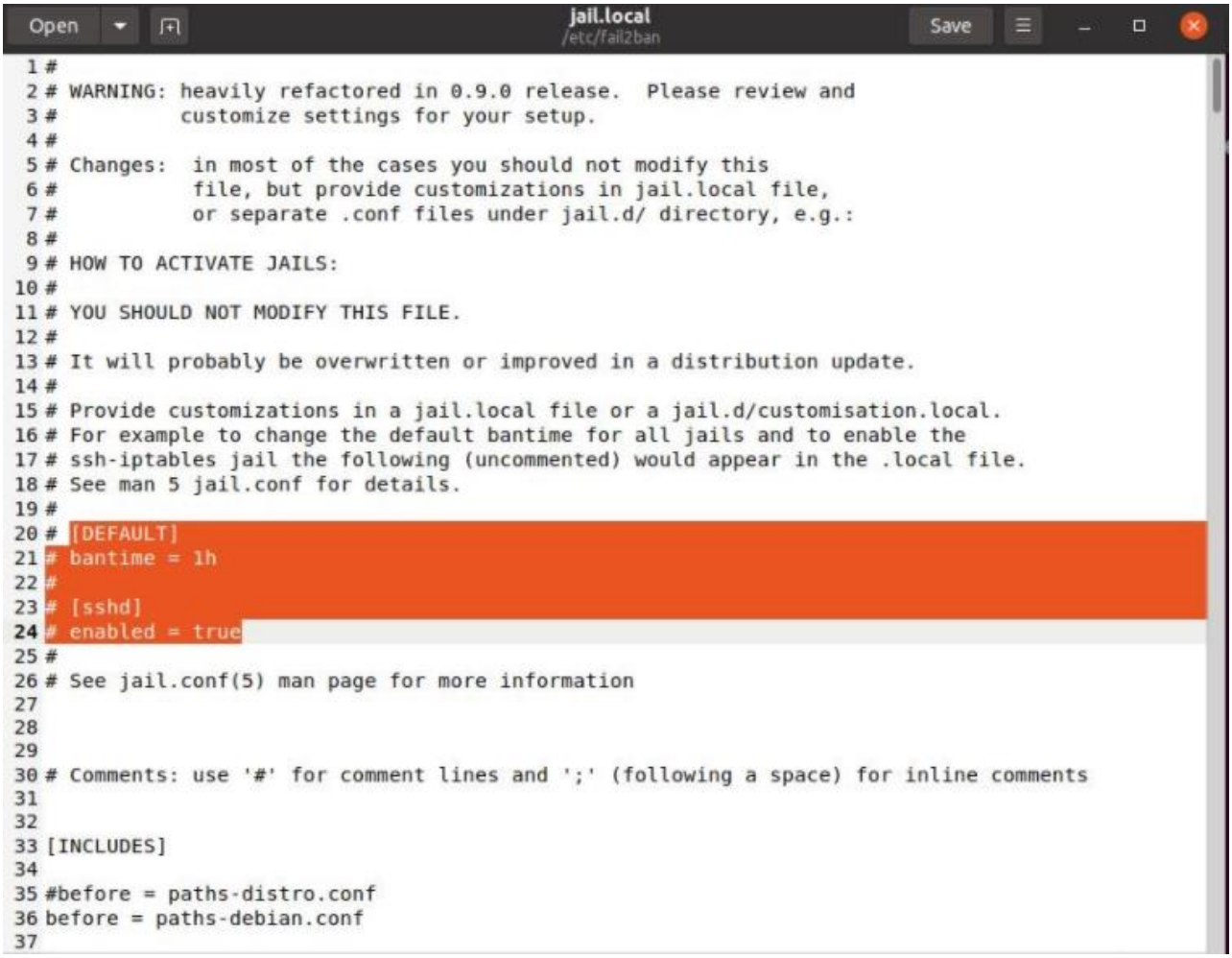

Рисунок 3.3 - Налаштування конфігурації ПЗ Fail2ban.

Якщо ви не хочете, щоб Fail2ban ігнорував кілька IP-адрес під час сканування, ви повинні вказати значення ігнорування та часу. bantime – цей

параметр визначає час у секундах, коли підозрюється IP. Спочатку його значення становить 10 хвилин Пошук - програма, яка визначає час у секундах, визначає, чи немає підозрілих дій. maxretry — це число, яке не вдалося досягти сервера. Якщо значення перевищено, IP буде вимкнено [40, с.34].

Нижче наведено список наших найпопулярніших служб, зокрема ssh, ftp тощо. Детальніше про те, як їх встановити, буде розказано в кінці цього розділу, в розділі «Налаштування Fail2ban». Після зміни в'язниці local.local переконайтеся, що ви запустили Fail2ban з інструкціями: Перш за все, налаштуйте захист VPS за допомогою SSH за допомогою Fail2ban. Для цього знайдіть частину [ssh] у в'язниці. Він повинен працювати особливим чином. Однак, якщо це необхідно, ви повинні переконатися, що значення параметра capable має значення true, а не false.

Вкажімо значення параметрів, на підставі яких Fail2ban повинен виконувати відстеження активності: filter - фільтр, який буде використовуватися. За замовчуванням це /etc/fail2ban/filter.d/sshd.conf; action - дії, які буде виконувати Fail2ban при виявленні атакуючої IP-адреси, всі правила реагування на дії зловмисника описані у файлі /etc/fail2ban/action.d. Відповідно, в якості значення параметра action не може бути вказана інформація, якої немає в файлі /etc/fail2ban/action.d; logpath - повний шлях до файлу, в який буде записуватися інформація про спроби отримання доступу до VPS. findtime - час в секундах, протягом якого спостерігається сайтів із підозрілою активністю; maxretry - дозволену кількість повторних спроб підключення до сервера; bantime - проміжок часу, протягом якого потрапив в чорний список IP залишатиметься заблокованим [31, с.164-166].

Варто звернути увагу на той факт, що зовсім необов'язково прописувати значення вищевказаних параметрів в кожній секції. Якщо їх не згадувати, в дію вступлять налаштування, зазначені в головному розділі [DEFAULT]. Головне, щоб для змінної enabled було зазначено значення true, а не false. Розглянемо застосування параметрів реагування більш детально. Приклад конфігурації Fail2ban на порту SSH: Запис вище означає, що, якщо виконано більше 3 невдалих спроб підключення до VPS через основні порти SSH, то IP-адреса, з якого

виконувалася авторизація, потрапить в бан на 10 хвилин. Правило заборони буде додано в iptables. У той же час власник сервера отримає повідомлення на e-mail, вказаний в значенні змінної dest, про те, що вказаний IP був заблокований за спробу отримання несанкціонованого доступу по протоколу SSH.

Висновки до розділу 3

Отже, багато компаній нехтують захистом своїх мереж від різних пристроїв, включаючи ноутбуки. Якщо в офіс приходить сторонній користувач і підключається до корпоративної мережі, система вважає з'єднання надійним. Такий пристрій може навіть досягати та сканувати місцеві труби. Або ноутбук може бути заражений, навіть якщо власник про це не знає. Все це згубно впливає на загальну структуру всієї системи.

Небезпечними можуть стати й IoT-пристрої, які широко використовуються в компаніях. Наприклад, американське казино зніс акваріум. Зловмисників підключили до датчика тепла води та перемістили в інші частини мережі для отримання інформації. Таким же чином хакери можуть використовувати незахищені відеокамери, пристрої відображення відео або системи миттєвого доступу.

Рішення — Network Access Control, підтримує реалізацію політики безпеки та покращує безпеку мережі. Роботодавці, які мають правильний доступ, можуть отримати легкий доступ до інформації за потреби.

ВИСНОВКИ

Через Інтернет зловмисники можуть викрасти захищені мережі та отримати важливу інформацію, тому нам потрібно докласти більше зусиль, щоб захистити наші мережі та підтримати їхню безпеку завдяки підвищенню безпеки.

У результаті дослідження та аналізу у численних наукових роботах виявлено протиріччя між діяльністю злочинців і DDoS-атаками, а також найкращий спосіб їх захисту. Багато з найбільш широко використовуваних методів запобігання DDoS-атак не можуть бути використані для боротьби з сучасними методами атак на родину. Такі рішення, як фільтрація або чорні діри, засновані на відхиленні вхідних і вихідних даних, значно знижують доступність мережі та завдають шкоди організаціям, а не заважають їм відмовлятися від послуг у довгостроковій перспективі.

Також важливо не знати про атаки керування мережею або використання мережевих служб. Знання фальшивих адрес працює з великою кількістю інформації, і шанси отримати джерело атаки невеликі. Крім того, блокування джерела атаки, а також фільтрація потоку транспорту вимагає блокування частини дороги. Багато великих організацій вирішують проблему відхилення послуг за межами мережевої комунікаційної мережі.

Ця відповідь підтверджує, що мережа має хорошу репутацію з несподіваним збільшенням навантаження на пресу, але вона вимагає великих економічних інвестицій, а також правильного використання ресурсів для отримання прибутку. У аналізі порівнюються сучасні стратегії захисту телекомунікаційних мереж щодо запобігання, виявлення та контролю можливих атак з урахуванням інформації про способи захисту національних та міжнародних експертів та результатів досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бутузов В. М. Співвідношення понять «комп'ютерна злочинність» і «кіберзлочинність» / В. М. Бутузов // Інформаційна безпека людини, суспільства, держави. – 2014. – № 1(3). – С. 16-18.

2. Карчевський М. В. Комп'ютерна інформація, як предмет злочину в сфері використання ЕОМ, систем, комп'ютерних мереж та мереж електрозв'язку / М. В. Карчевський // Боротьба зі злочинами у сфері комп'ютерної інформації : проблеми та шляхи їх вирішення : матеріали міжвуз. наук.-практ. конф. 14 груд. 2007 р. – Донецьк : Донец. юрид. ін-т, 2012. – С. 61-64.

3. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : [моногр.] / Карчевський М. В. – Луганськ : Луган. держ. ун-т внутр. справ, 2012. – 327 с.

4. Карчевський М. В. Основні напрями вдосконалення кримінально-правового забезпечення інформаційної безпеки / М. В. Карчевський // Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення : матеріали всеукр. наук.-практ. конф. 9 груд. 2013 р. – Донецьк : Донец. юрид. ін-т, 2013. – С. 54-58.

5. Кіберзлочинність та відмивання коштів [Електронний ресурс] / Департамент фінансових розслідувань. Державна служба фінансового моніторингу. – 2013. – Режим доступу: http://www.sdfm.gov.ua/content/file/Site_docs/2013/20131230/tipolog2013.pdf

6. Кримінальний кодекс України [Електронний ресурс] / Офіційний сайт Верховної Ради України. – Режим доступу: http:// zakon1.rada.gov.ua

7. Литвинов М. Деятельность управления по борьбе с киберпреступностью МВД Украины на современном этапе [Электронный ресурс]. – Режим доступу : http: //cybersafetyunit.com/deyatelnost-upravleniya-po-borbe-s-kiberstupnostyumvdna-sovrtmennom-etape/.– 01.07.2015/ 38

8. Марков В. В. Про механізми скоєння злочинів у кіберпросторі та особливості їх кваліфікації / В. В. Марков // Південноукраїнський правничий часопис. – 2013. – № 1. – С. 112-115.

9. Марков В. В. Статистичне дослідження показників кіберзлочинності: методологічний аспект / В. В. Марков // Право і безпека. – 2015. – № 2. – С. 136-140.

10. Марков В. В. Хакерські атаки на імплантати як один із способів протиправного використання кіберпростору: сутність та види / В. В. Марков // Вісн. Харк. Ун ту внутр. справ. – 2014. – № 2. – С. 139-147.

11. Меживой В. П. Способи оперативного виявлення несакціонованого втручання в роботу автоматизованих систем та комп'ютерних мереж / В. П. Меживой // Організація і тактика документування підрозділами ДСБЕЗ злочинів у комп'ютерних мережах та мережах електрозв'язку : матеріали всеукр. наук. – практ. конф., 4 груд. 2013 р. – Донецьк : Донец. юрид. ін-т, 2013. – С. 115-119.

12. Погорецький М. Кіберзлочини : до визначення поняття / М. Погорецький, В. Шеломенцев // Вісн. прокуратури. – 2012. – № 8. – С. 89-96.

13. Поляруш О. О. Використання мережі Інтернет як каналу інформаційнопсихологічного впливу / О. О. Поляруш // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ, 2015. – № 21. – С. 218-227.

14. Ращенко Є. Кримінально-правове забезпечення боротьби зі злочинами у сфері використання комп'ютерних технологій / Є. Ращенко // Право України. – 2013. − № 10. – С. 87-91.

15. Розенфельд Н. Віртуальний предмет злочинів, пов'язаних з порушенням авторського права і суміжних прав / Н. Розенфельд // Право України. – 2012. − № 5. – С. 105-109.

16. Рудик М. В. Суб'єкт злочину, передбаченого ст. 362 КК України / М. В. Рудик // Роль та місце ОВС у розбудові демократичної правової держави. – Одеса, 2012. – С. 323-324.

17. Сабадаш В. П. Интернет-мошенничество: понятие, структура и динамика разивтия / В. П. Сабадаш // Актуальные проблемы современной криминалистики. – Минск , 2010. – С. 136-143.

18. Сапальов В. П. Особливості огляду місця події при розслідуванні злочинів в комп'ютерній сфері / В. П. Сапальов // Організація і тактика документування підрозділами ДСБЕЗ злочинів у комп'ютерних мережах та мережах електрозв'язку : матеріали всеукр. наук. – практ. конф., 4 груд. 2013 р. – Донецьк : Донец. юрид. ін-т, 2013. – С. 179-182.

19. Сезонова І. К. Попередження неправомірних діянь при використанні інформаційних систем / І. К. Сезонова, Т. П. Колісник // Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук. практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 68-76.

20. Семенов Г. Криминалистическая классификация преступлений против информации в системе сотовой связи / Г. Семенов, Н. Карпов // Закон и жизнь. – 2015. − № 5. – С. 24-28.

21. Семенов Г. Система сотовой связи как основополагающий фактор, детерминирующий способы совршения мошеничества в системе сотовой святи // Г. Семенов, Н. Карпов // Закон и жизнь. – 2014. − № 3. – С. 20-24.

22. Сервецький І. В. Деякі проблеми захисту персональних даних в Україні / І. В. Сервецький, В. В. Редька // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ, 2014. – № 9. – С. 193-199.

23. Симкин Л. Как бороться с «сетевыми пиратами» / Л. Симкин // Рос. юстиция. – 2012. – № 7. – С. 62-64.

24. Скалозуб Л. П. Інтелектуалізація злочинності. Варіант стримування / Л. П. Скалозуб, В. М. Бутузов // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К. : МНДЦ, 2012. – № 1. – С. 295-307.

25. Скалозуб Л. П. Стан захисту інтелектуальної власності та протидії комп'ютерній злочинності: проблемні питання вирішення / Л. П. Скалозуб // Організація протидії у сфері інтелектуальної власності та комп'ютерних технологій : доповіді провідних вчених, представників громадськості, 40

державних службовців та працівників підрозділів ДСБЕЗ на міжвід. сем. – К., 2014. – С. 5-12.

26. Солодка О. М. Боротьба з комп'ютерною злочинністю як пріоритетний напрям забезпечення інформаційної безпеки України / О. М. Солодка // Актуальні проблеми управління інформаційною безпекою держави : зб. матеріалів наук.-практ. конф., 17 берез. 2010 р., м. Київ. – К. : Нац. акад. СБУ України, 2010. – С. 126-128.

27. Ставер А. В. Загальні вразливості банківських карт і способи їх усунення /А. В. Ставер // Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 144-147.

28. Струков В. М. Деякі технічні аспекти побудови кіберпростору в контексті протидії кіберзлочинності / В. М. Струков // Протидія кіберзлочинності в фінансово-банківській сфері : матеріали Всеукр. наук.-практ. конф., Харків, 23 квіт. 2013 р. – Х. : ХНУВС, 2013. – С. 65-68.

29. Струков В. М. Технічні аспекти побудови кіберпростору, що сприяють кіберзлочинності / В. М. Струков // Боротьба з інтернет-злочинністю : матеріалиміжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). – Донецьк : Донец. юрид.ін-т, 2013. – С. 234-235.

30. Якубівська Ю. Є. Світові тенденції розвитку кіберзлочинності / Ю. Є. Якубівська // Зовнішня торгівля: економіка, фінанси, право : Науковий журнал. Серія : Економічні науки. - К. : УДУФМТ, 2014. - № 5-6 (76-77). - С. 125-130.

31. Якубівська Ю. Є. Кібератаки у сфері інформаційної безпеки: тенденції на євразійському просторі / Ю. Є. Якубівська // Вітчизняна система охорони і захисту інтелектуальної власності в умовах приєднання до Європейського Союзу: Збірник тез доповідей Всеукраїнської науково-практичної конференції, м. Тернопіль, 24-25 квітня 2015 р., ТНЕУ. – Тернопіль, 2015. – С. 164-166.

32. Net Losses Estimating the Global Cost of Cybercrime [Electronic Source] / Center for Strategic and International Studies. – 2014/ - Режим доступу: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

33. Указ Президента України від 22.05.1998 № 505/98 «Про Положення про порядок здійснення криптографічного захисту інформації в Україні». [Електронний ресурс] // Законодавство України. – 1999. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/505/98.

34. О. Трофименко, Я. Дубовой, "Щодо правового потенціалу безпечного функціонування кіберпростору", Кібербезпека в Україні: правові та організаційні питання: матер. III всеукраїнської наук.-практ. конф., 30 листопада 2018 р., Одеса: ОДУВС, С. 5–7.

35. Владимирова Т. В. Сетевые коммуникации как источник информационных угроз / Т. В. Владимирова. // Социологические исследования. – 2011. – №5. – С. 123–129.

36. Галушка В. В. Алгоритм обнаружения сетевых атак на основе подмены ответов DHCP-сервера / В. В. Галушка, В. А. Баранцева // Инновационные технологии научного развития: сборник статей международной научно-практической конференции. / В. В. Галушка, В. А. Баранцева. – Казань: АЭТЕРНА, 2017. – (Инновационные технологии научного развития: сборник статей международной научно-практической конференции.). – С. 16–19.

37. Козьмовский Д. В. Методы анализа трафика и определения сетевой деятельности в вычислительных сетях в интересах контроля пользователей / Д. В. Козьмовский, В. И. Куватов, А. И. Примаков. // Вестник Санкт-Петербургского университета МВД России.. – 2014. – №1. – С. 112–115.

38. Галушка В. В. Методы и средства выявления сетевых атак на основе анализа транзитных пакетов / В. В. Галушка, Е. Д. Верхорубова. // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2016. – №9. – С. 298–303.

39. Методика выявления сетевых атак класса «Человек посередине» на основе анализа транзитного трафика [Електронний ресурс] / В. В.Галушка, В. А. Фатхи, Д. В. Фатхи, Е. Н. Чуйкова // Инженерный вестник Дона. – 2017.

40. Kiruthika Devi B. S., Subbulakshmi T. A. Comparative Analysis of Security Methods for DDoS Attacks in the Cloud Computing Environment. Indian Journal of

Science and Technology, 2016, vol. 9(34), pp. 1–7. DOI: 10.17485/ijst/2016/v9i34/93175.

ДОДАТОК А

Лістінг програми

WHOIS інформація про заблокованому IP. Приклад такого повідомлення від Fail2ban:

Hi,

The IP 61.147.103.113 has just been banned by Fail2Ban after

3 attempts against SSH.

Here are more information about 61.147.103.113:

% [whois.apnic.net]

% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html

% Information related to '61.147.0.0 - 61.147.255.255'

inetnum: 61.147.0.0 - 61.147.255.255

netname: CHINANET-JS

descr: CHINANET jiangsu province network

descr: China Telecom

descr: A12,Xin-Jie-Kou-Wai Street

descr: Beijing 100088

country: CN

admin-c: CH93-AP

tech-c: CJ186-AP

mnt-by: MAINT-CHINANET

mnt-lower: MAINT-CHINANET-JS

mnt-routes: maint-chinanet-js

changed: hostmaster@ns.chinanet.cn.net 20020209

changed: hostmaster@ns.chinanet.cn.net 20030306

status: ALLOCATED non-PORTABLE

source: APNIC

role: CHINANET JIANGSU

address: 260 Zhongyang Road,Nanjing 210037

country: CN

phone: +86-25-86588231

phone: +86-25-86588745

fax-no: +86-25-86588104

e-mail: ip@jsinfo.net

remarks: send anti-spam reports to spam@jsinfo.net

remarks: send abuse reports to abuse@jsinfo.net

remarks: times in GMT+8

admin-c: CH360-AP

tech-c: CS306-AP

tech-c: CN142-AP

nic-hdl: CJ186-AP

remarks: www.jsinfo.net

notify: ip@jsinfo.net

mnt-by: MAINT-CHINANET-JS

changed: dns@jsinfo.net 20090831

changed: ip@jsinfo.net 20090831

changed: hm-changed@apnic.net 20090901

source: APNIC

changed: hm-changed@apnic.net 20111114

person: Chinanet Hostmaster

nic-hdl: CH93-AP

e-mail: anti-spam@ns.chinanet.cn.net

address: No.31 ,jingrong street,beijing

address: 100032

phone: +86-10-58501724

fax-no: +86-10-58501724

country: CN

changed: dingsy@cndata.com 20070416

changed: zhengzm@gsta.com 20140227

mnt-by: MAINT-CHINANET

source: APNIC

% Information related to '61.147.0.0/16AS23650'

route: 61.147.0.0/16

descr: CHINANET jiangsu province network

country: CN

origin: AS23650

mnt-by: MAINT-CHINANET-JS

changed: ip@jsinfo.net 20030414

source: APNIC

% This query was served by the APNIC Whois Service version 1.69.1-APNICv1r0 (UNDEFINED)

Regards,

Fail2Ban

Рисунок 1 - Налаштування параметрів бана IP - адреси

Додатково для захисту SSH активуєму наступну секцію:

```
[Ssh-ddos]
enabled = true
port = ssh
filter = sshd-ddos
logpath = /var/log/auth.log
maxretry = 2
```

Ви можете використовувати комбінацію Netfilter / Iptables та IPsets для зберігання великого списку IP-адрес. Призначте Fai2ban таким чином, зробіть частини [ssh-iptables-ipset4]:

```
[ssh-iptables-ipset4]
enabled = true
port        = ssh
filter = sshd
action = iptables[name=SSH, port=ssh, protocol=tcp]
logpath = /var/log/auth.log
findtime = 300
maxretry = 3
bantime = 600
 [roundcube-auth]
enabled = true
filter = roundcube-auth
port        = http,https
logpath = /var/log/mail.log
action = iptables-multiport[name=roundcube, port="http,https"]
bantime = 86400
maxretry = 3
findtime = 3600
```

Для захисту сервера Apache можна використовувати такі налаштування Fail2ban:

```
[apache]
enabled = true
port    = http,https
filter = apache-auth
logpath = /var/log/apache2/error.log
maxretry = 3
[apache-multiport]
enabled = true
port    = http,https
filter  = apache-auth
logpath = /var/log/apache2/error.log
maxretry = 3
[apache-noscript]
enabled = true
port    = http,https
filter = apache-noscript
logpath = /var/log/apache2/error.log
maxretry = 3
[apache-overflows]
enabled = true
port    = http,https
filter = apache-overflows
logpath = /var/log/apache2/error.log
maxretry = 2
```

Для захисту FTP-сервера vsftpd за допомогою Fail2ban можна використовувати такі параметри:

```
[vsftpd]
enabled = true
port    = ftp,ftp-data,ftps,ftps-data
filter = vsftpd
```

logpath = /var/log/vsftpd.log

action = iptables[name=VSFTPD, port=21, protocol=tcp]

bantime = 600

maxretry = 3

findtime = 1800

На цьому установка Fail2ban завершена. З повним переліком правил, які будуть дотримуватися під час моніторингу на нашому VPS, ви можете ознайомитися за допомогою команди sudo iptables -L. Якщо IP-адреса Fail2ban заблокована помилково, ви можете видалити її з чорного списку за допомогою команди: sudo fail2ban-client set JAIL unbanip IP Де JAIL — ім’я jail. Частина файлу конфігурації, згідно з приватним законодавством. був зроблений блокування, IP - адреса, який потрібно розблокувати. Приклад команди розблокування: sudo fail2ban-client set ssh-iptables unbanip 61.147.103.113 [32].