Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: *"Удосконалення захисту веб-ресурсів Від DDoS-атак"*

Виконав: студент (ка)

Спеціальності:

125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)

		Грекул І.А.
	підпис	(прізвище та ініціали)
Керівник		*Загородна Н.В.*
	підпис	(прізвище та ініціали)
Нормоконтроль		
	підпис	(прізвище та ініціали)
Завідувач кафедри		*Загородна Н.В.*
	підпис	(прізвище та ініціали)
Рецензент		
	підпис	(прізвище та ініціали)

м. Тернопіль – 2021

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Грекулу Іллі Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Удосконалення захисту веб-ресурсів
Від DDoS-атак

Керівник роботи Загородна Н.В.., к.т.н., зав. каф. КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «16» 02 2021 року № 4/7-114

2. Термін подання студентом завершеної роботи 17.06.2021

3. Вихідні дані до роботи Статичні звіти,стасистики,описи,інформативні статті

4. Зміст роботи (перелік питань, які потрібно розробити)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Гурик О.Я., доцент кафедри МТ		

7. Дата видачі завдання 16.02.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.02 – 19.02	*Виконано*
2.	Підбір джерел про проблеми фішингу	20.02 – 27.02	*Виконано*
3.	Опрацювання джерел в галузі дослідження	28.02 – 16.03	*Виконано*
4.	Виконання дослідження щодо розробки програмного		
	Забезпечення щодо виявлення фішингових сайтів		
	на основі відкритих даних	17.03 – 29.03	*Виконано*
5.	Розроблення програмного коду		
6.	Оформлення розділу «Огляд літературних джерел»	30.03 – 12.04	*Виконано*
7.	Оформлення розділу «Теоретичні основи»	13.04 – 29.04	*Виконано*
8.	Оформлення розділу «Практична частина. Проектування		
	програмного забезпечення для виявлення фішингових вебсайтів»	30.04 – 13.05	*Виконано*
9.	Виконання завдання до підрозділу «Безпека		
	життєдіяльності, основи хорони праці»	14.05 – 21.05	*Виконано*
10.	Оформлення кваліфікаційної роботи	22.05 – 05.06	*Виконано*
11.	Нормоконтроль	06.06 – 12.06	*Виконано*
12.	Перевірка на плагіат	10.06 – 15.06	*Виконано*
13.	Попередній захист кваліфікаційної роботи	16.06 – 19.06	*Виконано*
14.	Захист кваліфікаційної роботи	23.06	

Студент _____ *Грекул І.А.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Загородна Н.В.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Удосконалення захисту веб-ресурсів від DDoS-атак // Кваліфікаційна робота ОР «Бакалавр» //Грекул Ілля Андрійович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-42 // Тернопіль, 2021 // С. 44 , рис. – 20, табл. – 0 , кресл. – 0, додат. – 1 .

Ключові слова: ВЕБ-РЕСУРС, АТАКА, DDoS, ВЕБСАЙТ, СТАТИСТИКА.

Кваліфікаційна робота присвячена удосконаленню захисту веб-ресурсів від DDoS атак. В роботі проведений порівняльний аналіз існуючих методів нападів та типів атак. Проаналізовані методи захисту та вибрані найкращі варіанти для реалізації.

В роботі також проведено DDoS-атаку на веб-ресурси. Для тесту було вибрано декілька програм та способів з різними типами атаки. Розібрані сильні та слабкі сторони DDoS-машин та потенційних жертв. Наведено статистику для усвідомленості проблеми та її стану в житті користувачів. Розроблено систему захисту та подальші рекомендації для його підтримки. Було отримано багато корисного досвіду та нової інформації яка допомогла в написанні КРБ.

ANNOTATION

Web-resources protection improvement against DDoS-attacks // Qualification thesis of educational level "Bachelor" // Grekul Ilya Andreevich// Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and software engineering, Department of Cybersecurity, СБс-42 group // Ternopil, 2021 // P. 44, fig. - 20, table. - 0 , chair. - 0, added. -1.

Keywords: WEB RESOURCE, ATTACK, DDoS, WEBSITE, STATISTICS.

Qualification work is devoted to improving the protection of web resources from DDoS attacks. The paper compares the existing methods of attacks and types of attacks. The methods of protection are analyzed and the best options for implementation are selected.

The work also carried out a DDoS attack on web resources. Several programs and methods with different types of attacks were selected for the test. The strengths and weaknesses of DDoS machines and potential victims are analyzed. Statistics are given to understand the problem and its state in the lives of users. A protection system and further recommendations for its support have been developed. A lot of useful experience and new information was gained which helped in writing the CRB.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

КРБ – Кваліфікаційна робота бакалавра;

ОС – Операційна система;

МЕ – Міжмережевий екран;

ДР-1 - Квоти;

ПО – програмне забезпечення;

ВСТУП

Сучасне суспільство вже не може обійтися без технологій тому, що технології проникли та оточують нас у всіх сферах життя. Особливо невід’ємною частиною життя є глобальна мережа Інтернет. Сьогодні одним з головних завдань є забезпечення безпеки інформації людей в самій мережі.

Захист веб-ресурсів залишається одним із важливих напрямків інформаційної безпеки. Щороку кількість веб-ресурсів росте разом з кількістю конфіденційної інформації, що локалізується на серверах віддаленого доступу із використанням «хмарних» технологій. Тому зростає не тільки кількість нападів, а ще великий вплив на економічний та політичний стан.

В даний час, в Україні, в зв'язку з входженням у світовий інформаційний простір, швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій. Системи телекомунікацій активно впроваджуються у фінансові, промислові, торгові і соціальні сфери. У зв'язку з цим, різко зріс інтерес широкого кола користувачів до проблем захисту інформації. Тривалий час методи захисту інформації розроблялися тільки державними органами, а їхнє впровадження розглядалося як виключне право тієї або іншої держави. Проте, в останні роки, з розвитком комерційної і підприємницької діяльності збільшилась кількість спроб несанкціонованого доступу до конфіденційної інформації, а проблеми захисту інформації виявилися в центрі уваги багатьох вчених і спеціалістів із різноманітних країн.

Таким чином удосконалення систем захисту та їх систем залишається актуальною проблемою, особливо враховуючи постійне удосконалення інструментів атак і створення нових методів.

Мета КРБ - аналіз інформації, що стосується питань рівня безпеки веб-ресурсів, узагальнення та розробка відповідних варіантів захисту.

Для досягнення мети було поставлено такі завдання та цілі:

- Написати сайт для тестування та проводження досліджень.
- Проаналізувати та виявити основні вразливості.
- Виявити недоліки протоколів.

- Реалізувати атаку для подальшого пошуку вразливостей
- Виявити ефективний захист та реалізувати його.

Об’єкт досліджень – сайт «DarkSpace».

Під час роботи було використано наступні методи дослідження:

- Аналіз
- Моделювання та експеримент
- Наукове дослідження

Об’єкт дослідження - методика тестування на проникнення веб-додатків.

Предмет дослідження є вразливості веб-серверів, методи їх виявлення та знешкодження.

Практичне значення завдання – практичний захист веб-ресурсу від атак.

1 ДОСЛІДЖЕННЯ МОЖЛИВИХ СПОСОБІВ ЗАХИСТУ ТА СТАТИСТИКА ВРАЗЛИВОСТЕЙ

1.1 Дослідження можливих способів захисту

Провідною метою створення захисту є збереження цінних даних компанії чи користувача від зловмисників. Зараз є цілі компанії які зосереджені тільки на цій задачі.Вони створюють нові способи захисту від атак, інформують компанії та потенційниз жертв про ризики та дають безкоштовну інформацію про загрози та їх способи вирішення.

1) Переповнення буфера (buffer overflows)

Атака на переповнення буфера ґрунтується на пошуку програмних або системних вразливостей, здатних викликати порушення кордонів пам'яті та завершити додаток або виконати довільний бінарний код від імені користувача, під яким працювала вразлива програма.

Способи боротьби з атаками подібного типу:

1. Корегування вихідних кодів програми для усунення вразливостей.
2. Використання нездійсненних буферів.
3. Застосування перевірок цілісності.

3) Використання спеціалізованих програм

Робочі станції дуже уразливі для вірусів. Вірусами називаються шкідливі програми, які впроваджуються в інші програми для виконання небажаної дії.

Використання антивірусів і регулярне оновлення їх може вирішити проблему з вірусами але не допоможе проти сніфферов і rootkit-ів.

Шифрування даних не вирішує проблему сніфферов до кінця, проте, противник перехоплює дані, які не можна вільно прочитати. Для їх розшифровки потрібен час. Слід використовувати антисніффери (наприклад, AntiSniff або PromiScan), міжмережеві екрани та антируткіти.

4) Мережева розвідка

Мережевою розвідкою називається збір інформації про мережу за допомогою загальнодоступних даних і додатків.

Способи боротьби з цією атакою:

- Відключення відлуння ICMP і луна-відповідь на периферійних маршрутизаторах.
- Використання систем виявлення вторгнень (IDS).
-

5) IP-спуфінг

IP-спуфінг відбувається, коли зловмисник, що знаходиться всередині корпорації або поза нею видає себе за санкціонованого користувача.

Загрозу спуфінгу можна послабити (ні в якому разі не обійти) за допомогою таких заходів:

Контроль доступу. Найпростіший спосіб запобігання IP-спуфінгу полягає в правильному підборі управління доступом. Щоб знизити ефективність IP-спуфінгу, налаштуйте контроль доступу на відсікання будь-якого трафіку, що надходить із зовнішнього мережі з вихідним адресом, який повинен розташовуватися всередині вашої мережі. Якщо санкціонованими є і деякі адреси зовнішньої мережі, даний метод стає неефективним .

6) Атака типу man-in-the-middle

Ця атака відбувається, коли зловмисник перехоплює надіслані пакети даних, тобто зловмисник перехоплює дані надіслані звичайним користувачем. Існує тільки один спосіб захиститися від цієї атаки - шифрувати всі дані, що передаються мережею.

7) SQL-ін'єкція

SQL-ін'єкція - це атака, в ході якої змінюються параметри SQLзапитів до бази даних. Способи захисту від даної атаки (використовуються виключно адміністраторами ресурсів):

Для цілих і дробових величин, перед їх використанням в запиті досить привести величину до потрібного типу .

8) PHP-ін'єкція

Ця атака полягає в тому, що зловмисник вставляє злоякісний PHP-код в сайт. Способи боротьби з цією атакою (використовуються виключно адміністраторами ресурсів):

Перевіряти, чи не містить змінна $name (в нашому прикладі) сторонні символи:

9) Міжсайтовий скриптинг або XSS-атака

XSS атака - це вразливість, яка дозволяє впровадити в HTML-сторінку, що генерується сервером, якийсь довільний код, в якому може бути взагалі все що завгодно і передавати цей код в якості значення змінної, фільтрація по якій не працює, тобто сервер не перевіряє дану змінну на наявність в ній заборонених знаків -, , ', ".

Способи боротьби з даним видом атак (використовуються виключно адміністраторами ресурсів):

1. Заборонити включення безпосередньо параметрів $ _GET, $ _POST, $ _COOKIE в HTML-сторінці що генерується.

2. Заборонити завантаження довільних файлів на сервер, щоб уникнути завантаження шкідливих скриптів.

3. Всі завантажені файли зберігати в базі даних, а не в файловій системі.

10) XPath-ін'єкція.

XPath-ін'єкція - вид вразливостей, який полягає у впровадженні XPath-виразів в оригінальний запит до БД XML.

Способи боротьби з цією атакою (використовуються виключно адміністраторами ресурсів):

1. Перевірка коректності. Незалежно від програми, середовища або мови необхідно дотримуватися наступних практичних правилами:

- Припускайте, що всі дані що вводяться сумнівні.
- Перевіряйте дані як на стороні клієнта, так і на стороні сервера, оскільки перевірку на стороні клієнта надзвичайно легко перехитрити.
- Дотримуйтесь послідовної [missing word] стратегії захищеності додатку, ґрунтуючись на передовому досвіді розробки захищених додатків
- Тестуйте додаток на відомі загрози перед його випуском .

2. Перевірка даних на Web-сервері.

11) Відмова в обслуговуванні (DoS- і DDoS- атаки)

Атака DoS робить мережу недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або програми.

Загроза атак типу DoS може знижуватися трьома способами:

- Функції анти-спуфінга. Правильна конфігурація функцій анти-спуфінга на маршрутизаторах і міжмережевих екранах допоможе знизити ризик DoS.
- Функції анти-DoS. Правильна конфігурація функцій анти-DoS на маршрутизаторах і міжмережевих екранах може обмежити ефективність атак. Ці функції часто обмежують число напіввідкритих каналів в будь-який момент часу.
- Обмеження обсягу трафіку (traffic rate limiting). Організація може попросити провайдера обмежити обсяг трафіку. Цей тип фільтрації дозволяє обмежити обсяг некритичного трафіку, що проходить по вашій мережі.

Алгоритм упорядкування правил фільтрації мережевої трафіку

Міжмережеві екрани (МЕ) - невід'ємний елемент забезпечення мережевої безпеки. Застосування МЕ при побудові систем захисту інформації є не тільки частою практикою, а й обов'язковою вимогою ряду нормативних документів в області інформаційної безпеки. Політика міжмережевого екранування (визначення того, які мережеві потоки повинні бути пропущені, а які заблоковані) реалізується в МЕ набором правил фільтрації мережевого трафіку.

Структура представлення наборів правил фільтрації переважної більшості сучасних МЕ є лінійний список. Для кожного пакета, що проходить через МЕ здійснюється послідовний перебір правил з даного лінійного списку. Після знаходження першого правила фільтрації, яке повністю задовольняє відповідний мережевий пакет, перебір наступних в списку правил зупиняється. Таким чином, чим вище за списком буде стояти відповідне правило фільтрації, тим швидше МЕ прийме рішення про обробку мережевого пакета. Очевидно, що чим вище за списком будуть розташовуватися найбільш часто спрацьовані правила фільтрації, тим менше ресурсів МЕ буде витрачатися на послідовний перебір лінійного списку правил. У свою чергу, від інтенсивності використання обчислювальних ресурсів МЕ багато в чому залежить його пропускна здатність.

Запропонований алгоритм впорядкування правил фільтрації мережевого трафіку, дозволяє впорядковувати правила фільтрації в наборах правил за частотою їх спрацьовування. Мета - помістити найбільш часто використовувані правила на вершину списку, щоб мінімізувати витрачання ресурсів системи на послідовну перевірку великої кількості правил. Шляхом оптимізації даного процесу можлива істотна економія машинного часу і зниження навантаження на пристрої, що здійснює функції брандмауера.

Основу алгоритму становить технологія пасивного аналізу мережевого трафіку. Вона дозволяє побудувати статистичну модель трафіку, який проходить через МЕ і на її основі розрахувати частоту спрацьовування кожного правила фільтрації з набору правил. Блок-схема алгоритму представлена на рис. 1.1.

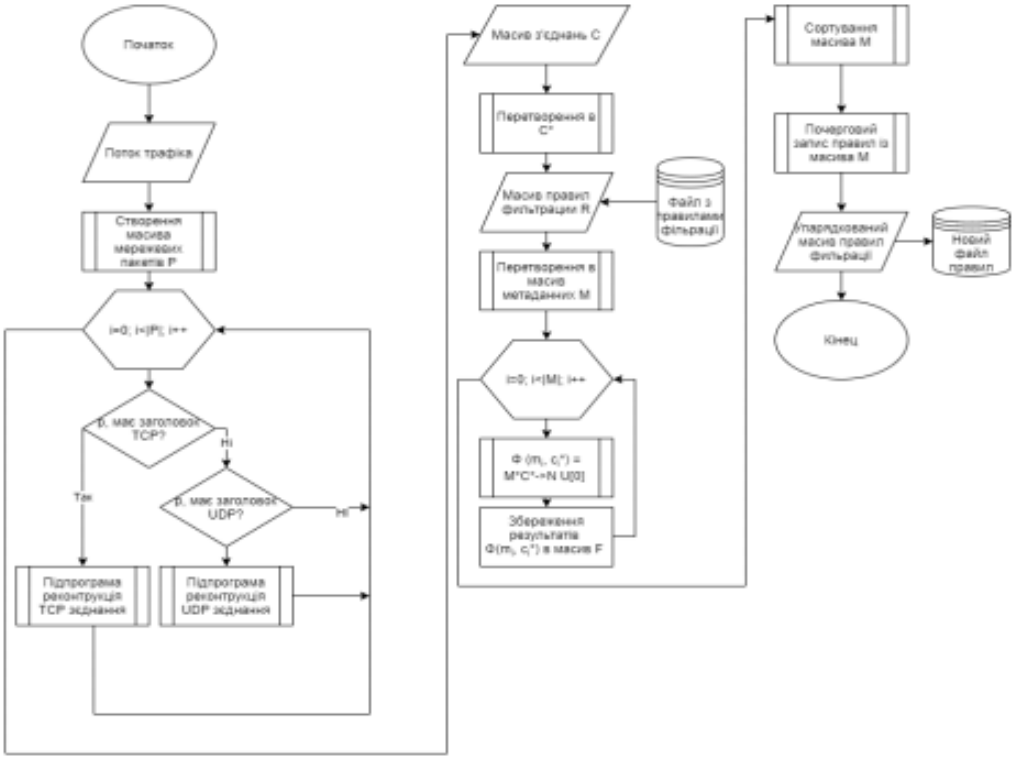

Рисунок 1.1 - Блок-схема алгоритму впорядкування правил фільтрації на основі статистичного аналізу

Ще одним вхідним параметром алгоритму є масив правил фільтрації брандмауера R, який необхідно впорядкувати. Значення даного масиву передаються в функцію перетворення в метадані, де здійснюється формування масиву метаданих M. Для кожного правила з R в масив M зберігається наступна інформація: порядковий номер, IP-адреса клієнта, IP-адреса сервера, який використовується протокол транспортного рівня, номер порту сервера, відповідне текстове представлення відповідного правила фільтрації. Далі масив метаданих M і зведений масив мережевих з'єднань C* надходять на вхід функції розрахунку значення Ф(m, сі *). В даній функції для кожного правила яке є належить до M на підставі зведеного масиву мережевих з'єднань C* здійснюється розрахунок функції Ф, значенням якої є невід'ємне ціле число, яке дорівнює кількості спрацьовувань відповідного правила:

$rj \in R: Ф: M \times C^* \rightarrow N \cup \{0\}$

На основі значень функції Ф процедура сортування здійснює пошук такої перестановки елементів масиву M, при якій відповідні їм значення функції Ф

розташовуються в порядку зменшення: Ф (mi) ≥ Ф (mj) ≥ ... ≥ Ф (mk). А на основі даної перестановки вже здійснюється формування впорядкованого масиву правил R.

Таким чином, застосування алгоритму впорядкування правил фільтрації міжмережевих екранів в наборах правил фільтрації дозволяє знизити навантаження на апаратну складову міжмережевих екранів і тим самим підвищити їх пропускну здатність. При цьому ефект від упорядкування правил буде найбільш помітний на високонавантажених міжмережевих екранах з великою кількістю використовуваних правил фільтрації (тисячі і десятки тисяч правил).

1.2 Статистика воазливостей

Найбільше атак проводиться на веб-ресурсах компаній у IT схерах. Збірка найпоширеніших атак зібрана та зображена на рисунку 1.2.

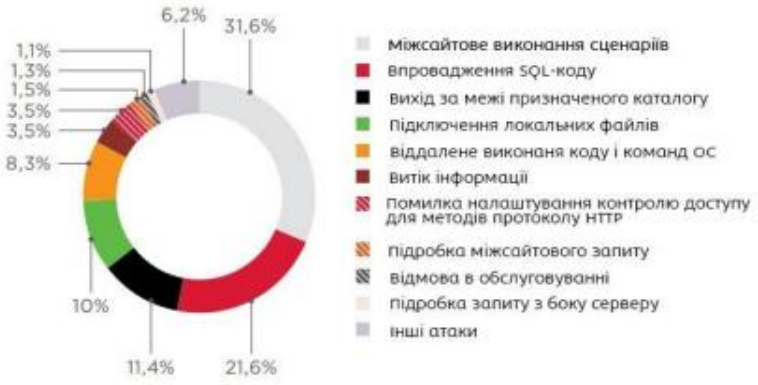

Рисунок 1.2 – Найпоширеніші атаки протягом року.

Серед найбільш популярних інтернет-нападів можна відзначити ті, які спрямовані на користувачів, а зокрема атаку «міжсайтове виконання сценаріїв», яка склала майже третину від загального числа та інші.

Виявлені атакі здійсюються переважно з російських IP-адрес. Це пов’язано з тим, що велика частина пілотних проектів проводиться для

російських компаній. У п’ятірку джерел увійшли США, Франція, Китай і Німетчина. Статистику джерел веб-атак можна побачити на рисунку 1.3.

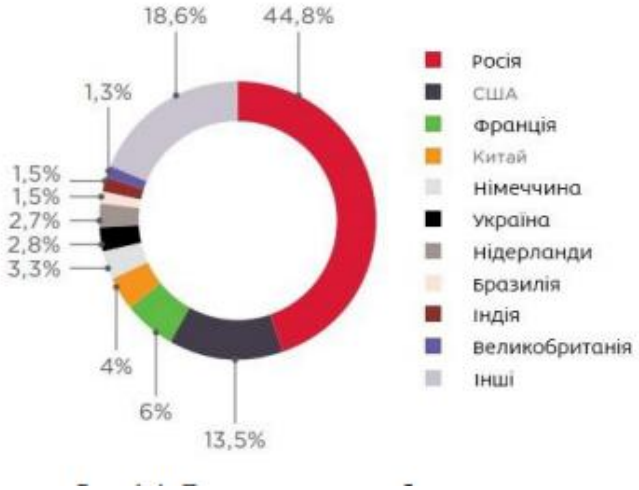

Рис 1.3 – Джерела атак на веб-додатки

1.3 Статистика по галузям

Сьогодні все більше стає як зловмисників, як і атак, які націлені на різні компанії з наміром нашкодити та причинити збитки. Компанії витрачають кошти для боротьби з хакерами.

Якщо взяти статистику нападів на сфери праці, то промислові і енергетичні підприємства постраждали найманше. Рівень зацікавленості на дане підприємство зрозуміле.Адже промислові компанії не мають такого впливу як IT-компанії. Статистика наведена на рисунку 1.4.

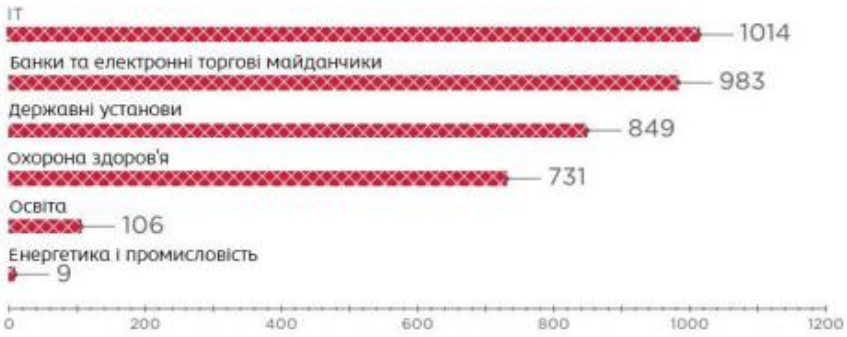

Рисунок 1.4 – Середнє число атак в день на веб-додаток однієї компанії.

Протягом року на веб-ресурси банків проводились численні атаки для знешкодження та виявлення помилок для того щоб в подальшому отримати вигоду чи просто деактивувати роботу банку на певний період. Як видно на статистиці, кількість атак зростає паралельно з активністю використання та проведення операцій клієнтів банку. Статистика зображена на рисунку 1.5.

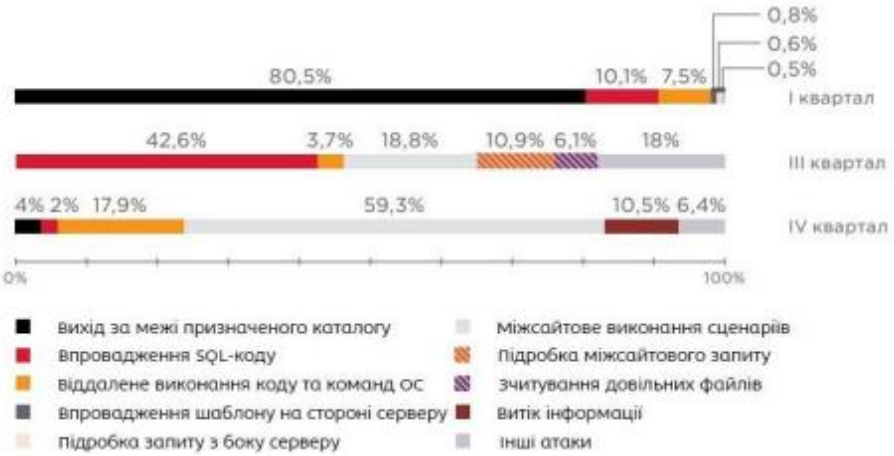

Рисунок 1.5 – Топ-5 атак на веб-додатки банків і електронні торгові майданчики.

Веб- ресурси освітніх установ страждають не так сильно як перечислені зверху. Беручи до уваги те, що такі сайти не мають сильного захисту. Їхніми нападниками частіше являються учні як хочуть повеселитись чи змінити свої оцінки в базі школи чи навчального закладу. Статистика наведена на рисунку 1.6.

Рисунок 1.6 – Топ-5 атак на веб-додатки в сфері охорони здоров’я.

В IT- сферах значну частину атак становлять напади типу «SQL-ін’єкція», «Підключення локальних файлів» «Вихід за межі призначеного каталогу» та «Віддалене виконання коду». Атаки на IT- компанії пов’язуються з поширенням шкідливого ПЗ, посиланням диз-інформації, завади створенню проектів та роботи,

У червні 2017 року пройшла масштабна кібератака за участю шифрувальника NotPetya. Жертвою опинилась бухгалтерська компанія яка розробляє ПЗ, яке і стало джерелом масового зараження. Восени код був виявлений в відомій утиліті CCleaner та опрелюднена на сайті виробника. Використання ресурсів IT-компаній вигідне для хакетів для розміщення свого шкідливого ПЗ , тому що з’єднання з IT-компаніями не викликає підозри для користувачів. Стастика атак на IT-компанії наведена на рисунку 1.7.

Рисунок 1.7 – Топ-5 атак на веб-додатки IT-компаній.

Висновки до першого розділу

Проаналізовано найпопулярніші напади на веб-ресурси та розглянуто їх вразливості, які можуть бути направлені для створення шкоди.

Досліджено та переглянуто вразливості які можуть бути провідними для реалізації атак а також розглянута статистика.

2 СТВОРЕННЯ САЙТУ ТА АНАЛІЗ ЗАГРОЗ НА ВЕБ-РЕСУРСИ

2.1 Створення сайту

Перед тим як приступати до головної задачі, потрібно створити тренувальне поле, тому першим кроком буде створення сайту.

Даний сайт не буде мати особливих відмінностей та спеціально спрощений для більшої кількості можливих вразливостей.

Сайт «GameShop» відноситься до інтернет-магазину.

Сайт орієнтований на англомовного користувача.

Сайт виконує такі функції:

- просвітницьку;
- рекламну;
- сервісну;
- комерційну;

Сайт містить користувацьку частину:

- Перегляд новин
- Перегляд товарів
- Авторизація
- Реєстрація

Структурна схема сайту зображена на рисунку 2.2

Рисунок 2.1 – Структурна схема головної сторінки сайту

Даний web-сайт містить наступні web-сторінки:

- Головна – для першого входу на сайт, та перегляду основної інформації про сайт та інше;

- Каталог – для перегляду товарів;

- Сторінка товару – для перегляду інформації про товар;

- Корзина – для перегляду товарів доданих в корзину;

- Сторінка авторизації – для авторизації на сайті;

- Сторінка реєстрації – для реєстрації на сайті.

Етапи створення сайту.

Створення сайту умовно можна розділити на такі етапи:

1. Попередній етап розробки сайту. На цьому етапі розв'язуються питання загального характеру. Обговорюється загальна концепція сайту, формуються та фіксуються цілі створення сайту.

2. Етап проектування сайту. Визначення структури сайту: меню, посилання, розміщення модулів, побудова списку компонентів, що підключаються, тощо.

3. Етап розробки й тестування сайту

4. Розміщення сайту

5. Розвиток ресурсу.

Можна виділити такі варіанти створення веб-сайтів(див.рис 2.3).

Рисунок 2.2 – Типи створення сайту

Коли створений дизайн сайту, коли готові всі функціональні модулі й компоненти, необхідно з'єднати всі елементи в єдине ціле, тобто зверстати сайт.

Верстка сайту - це кінцевий етап розробки сайту, створення структури сайту, що буде визначати відображення тексту й графіки на сайті в різних браузерах.

Для даного web-сайту була створена база даних «darkspace». В базі даних була розроблена таблиця для зберігання даних про користувачів, таблиця зберігає індикатор користувача, ім’я та прізвище, електронну пошту, пароль та статус; game –відповідає за всю інформацію про товар; photo – відповідає за зберігання відео та фото товарів; geners – відповідає за зберігання жанрів товарів;carusel – відповідає за виведення зображень на карусель.

Усі таблиці створені за допомогою SQL запитів в phpmyadmin.

PhpMyAdmin – це веб-додаток з відкритим кодом на мові PHP із графічним веб-інтерфейсом для адміністрування бази даних MySQL. Phpmyadmin дозволяє через браузер здійснювати адміністрування сервера MySQL, запускати запити SQL, переглядати та редагувати вміст таблиць баз даних.

2.2 Аналіз загроз на веб-ресурси

Атака під назвою DoS – зловмисний напад спрямований на завдавання шкоди веб-ресурсам способом генерування великих кількостей пакетів або запитів які перевантажують роботу системи. Для DDoS-атаки нападник створює безліч зламаних або контрольованих пакетів,запитів або джерел.

На початку розвитку мережевих технологій, DDoS використовувався лише для хороших цілей та був основним елементом для тестування пропускної та покращення, проте знайшлись люди які вирішили використовувати даний метод для своїх цілей . Атака DoS, яку також називають як «відмова в обслуговуванні», є одним з інструментів злодіїв вже більше 20 років і її популярність все збільшується разом з новими можливостями. Зараз виділяються такі основні цілі, якими керуються зловмисники:

- Шахрайство

Нападники захоплюють мережі чужих комп’ютерів та організовують атаки, які блокують роботу систем. Без встановлення захисту на комп’ютер чи мережу хакер може повністю зупинити роботу системи і шантажувати жертв для розблокування. Часто буває так, що цінність даних перевищує ціну, тому люди погоджуються на умови злодіїв.

- Розвиток або забава

Останнім часом DDoS-атаки цікавлять все більше людей і вони все частіше переходять на темну сторону хакерів як для забави, так і для власного досвіду чи розвитку.

- Конкуренція

В даний момент досить популярною є послуга DDoS атаки на замовлення. Конкуренти формують завдання для хакера, щоб знищити компанію-конкурента чи їхнє майно.

Основні види DDoS атак:

- Напад на перевищення ліміту системних джерел.

Дії, націлені на вичерпання запасів таких як оперативна і фізична пам’ять, процесорний ресурс.

- Недостатня перевірка даних користувача.

Перевірка даних може привести до тривалого або вічного циклу їх обробки, що призводить до підвищеного споживання ресурсів чи обсягів пам’яті.

- Штурм другого ряду.

Атаки які націлені на ділянки мережі в яких неправильно ввімкнено або налаштовано на системний захист який призводить до недоступності конкретних ресурсів.

- HTTP-флуд.

Надсилання великих http-пакетів, які заставляють сервер у відповідь відсилати пакети у відповідь, які мають значно більші розміри. Зловмисник має велику нагоду нанести велику шкоду жертві безглуздими пакетами, через які

сервер падає. Щоб відповідні пакети не входили в список заборонених, хакер змінює мережевий адрес у вузлі мережі на легітимний.

- ICMP-флуд (Smurf-атака).

Найнебезпечніший вид атаки. По широкомовній адресі злодій відправляє підроблений ICMP-пакет, в якому адреса відправника змінюється на адресу жертви. Вузли, які отримали цей пакет посилають відповідь на цей запит. Цей вид атаки зазвичай використовується з великою мережею для того, щоб безвідмовно знешкодити жертву.

- UDP-флуд (атака Fraggle).

Атака є аналогом ICMP флуду, проте замість цих пакетів використовуються пакети UDP. На порт жертви відправляються команди echo по широкомовному запиті. Після підміняється адреса на адресу жертви, яка отримує безліч повідомлень у відповідь.

- SYN-флуд.

Атака зосереджена на спробі запуску одночасних TCP-з’єднань через відправлення пакетів SYN з зворотнім зв'язком якого не існує.Через те що, потік цих пакетів надто великий, черга виявляється переповненою. Схема даної атаки наведена на рисунку 2.3.

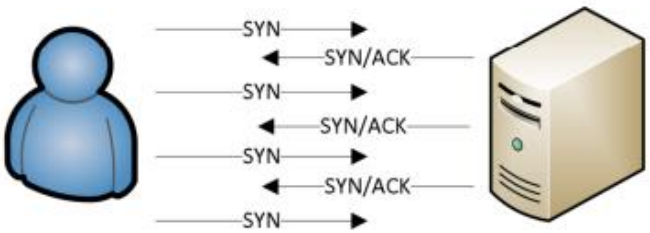

Рисунок 2.3 – SYN-флуд

- Відсидання важливих пакетів.

Злодій посилає пакети які не заповнюють смугу пропускання а витягують весь його ресурс. Відповідним чином в системі відбувається несправність і користувач не може отримати доступ до необхідних ресурсів.

- Заповнення сервера лог-файлами.

При неправильній ротації лог-файлів і неправильно встановленій системі квотування зловмисник може відправляти великі за об'ємом пакети, які незабаром займуть усе місце на жорсткому диску сервера.

- Помилки програмного коду.

Досвідчені організатори DDoS атак, повністю розібравшись в структурі жертви, пишуть програми-експлоїти, які дозволяють атакувати складні системи комерційних підприємств і організацій.

- Недоліки в програмному коді.

Зловмисники шукають помилки в програмному коді яких-небудь програм або ОС і примушують їх обробляти винятки, які вони обробляти не вміють, що призводить до падіння ядра або знешкодження усієї системи в цілому.

За даними статистики найпопулярніший тип атаки - HTTP-Flood (80%). Зараз хакери мають безліч технології для проведення даного нападу. У 54% комп’ютери ботнету посилають данні конкретній сторінці веб-ресурсу. Наступне місце (22%) - атака на поля авторизації. Третє місцу (13%) - атака спрямована на велику кількість завантаження файлів з веб-ресурсу.

На наступних місцях атаки типу UDP-Flood , SYN-Flood , ICMP-Flood. Описана статистика зображена на діаграмі - рис. 2.4

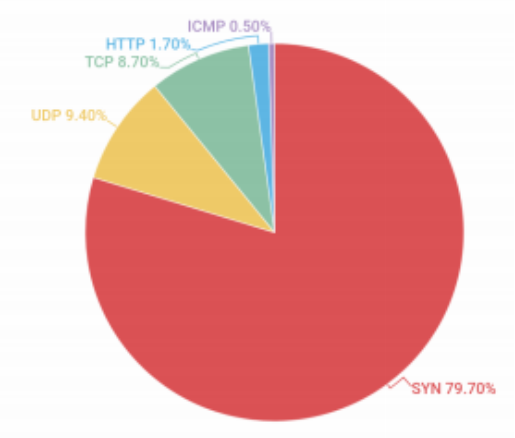

Рисунок 2.4 – Типи DDoS атак за популярністю.

Зазвичай мережа злодія (Кластер DDoS), з якої відбувається атака має три рівні - верхній рівень (комп’ютери з яких ведеться початок атаки), другий рівень

(десятки комп’ютерів які надають сигнали), третій рівень (ботнет). Структура зображена на рисунку 2.5

Рисунок 2.5 – Структура ботнет мережі

Майже всі веб-додатки містять вразливі місця які дозволяють злодіям діяти., тому що з кожним роком вразливості на веб-ресурсах збільшуються.

Зловмисники кожного разу обходять системи захисту веб-ресурсів чере що компнаії по захисту повинні створювати нові методи для протидії хакерам. У 19% всіх веб-ресурсів було знайдено критичні помилки що дозволяють отримати доступ навіть до ОС сервера. Це великі цифри для сьогодення і велика проблема для компаній, через що над вирішенням проблем працює велика кількість людей. На рисунку 2.6 наведений рівень захищеності веб-ресурсів.

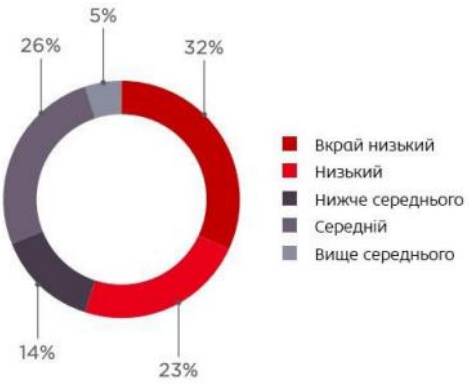

Рисунок 2.6 – Рівень захищеності

У 19% веб-додатків є вразливості, що дозволяють зловмиснику отримати контроль над самим додатком та ОС серверу. Якщо сервер знаходиться на периметрі мережі організації, зловмисник може проникнути у внутрішню мережу компанії. Як показують результати нашого дослідження вразливостей корпоративних інформаційних систем, 75% векторів проникнення в ЛОМ пов'язані з недоліками захисту веб-додатків.

У більшості випадків веб-додатки уразливі через помилки в коді. Змінами в конфігурації можуть бути усунені лише 17% вразливостей, причому більшість з них мають низький рівень ризику. Для усунення критично небезпечних вразливостей, як правило, потрібно вносити правки в код.

Кожен другий витік може привести до розголошення облікових даних, в тому числі для доступу до сторонніх ресурсів. Як приклад можна привести доступні всім користувачам конфігураційні файли, в яких зберігаються паролі.

Зловмисник може викрасти персональні дані користувачів в 18% веб-додатків, де здійснюється їх обробка. При цьому важливо відзначити, що персональні дані зберігаються і обробляються майже в кожному веб-додатку (91%).

В середньому на один веб-додаток припадає 33 уразливості, шість з яких мають високий рівень ризику. Число критично небезпечних вразливостей, яке припадає на один веб-додаток, в порівнянні з 2017 роком зросло в 3 рази.

Продуктивні системи містять менше вразливостей, ніж тестові, але це не робить їх більш захищеними. Частка продуктивних систем, що містять хоча б одну уразливість високого рівня ризику, більше, ніж тестових. Як показує практика, для успішного злому веб-додатку часто досить однієї критично небезпечної уразливості.

Аналіз вихідного коду підвищує ефективність перевірки. При наявності у експертів доступу до вихідного коду середнє число виявлених вразливостей високого рівня ризику, за статистикою, зростає більш ніж в два рази.

3 РЕАЛІЗАЦІЯ ВЕБ-АТАКИ ТА РОЗРОБКА ЗАХИСТУ

Метою даного розділу є реалізація різних методів атак на веб-ресурс для вибору найкращого захисту . В розділі буде описано як реалізовано атаки на веб-ресурс, та спрямування атак на нього. Для порівняння наведені два сайти.

3.1 Реалізація атак на веб-ресурс

Найпростіша атака для якої не потрібно багато зусиль чи ресурсів – це атака через командний рядок Windows.

Для реалізації DDoS атаки через командний рядок необхідно створити файл типу «.bat», та розпочати його редагування (Зображено на рисунку 3.1).

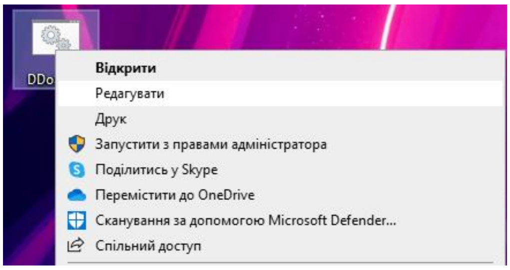

Рисунок 3.1 – файл «.bat»

Коли відкрилось вікно схоже на звичайний блокнот, потрібно ввести просту поманду, а саме : ping 127.0.0.1 -t –l 1000, де ping- команда обміну пакетами даних, -t – безперервна передача пакетів, -l – розмір поля даних в байтах, 127.0.0.1 – IP адреса сайту (в данному випадку адреса локального серверу). Процес виконання зображено на рисунку 3.2.

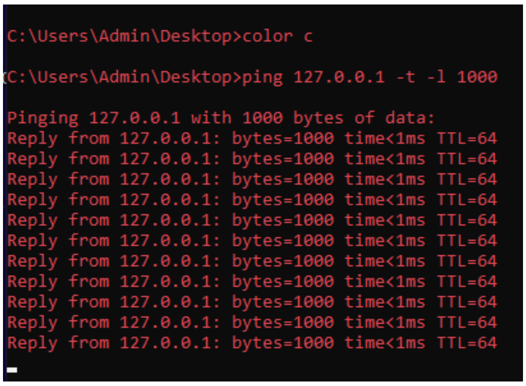

Рисунок 3.2 – Результат DDoS атаки через командний рядок.

Звичайно що така атака не буде успішною чи повноцінною, тому що обмін даними вдбувається між одним клієнтом та сервером. Проте якщо зробити це через декілька сотень чи тисяч клієнтів на один сайт, то атака буде вдалою.

Реалізація атаки через сторонню програму

Для проведення дослідів вибрано наступні программи : LOIC та Fastream Web Stress Test.

The Low Orbit Ion Cannon (LOIC) Низько орбітальна іонна гармата. Можливо найпопулярніша DDoS програма. Вона може розсилати масові запити по протоколам ICMP, UDP тим самим забиваючи канал до сервера жертви. Найвідоміша атака за допомогою LOIC була здійснена групою Anonymous в 2009 році і спрямована проти PayPal, Visa, MasterCard в помсту за відключення WikiLeaks від системи збору пожертвувань. Встановити на свій страх і ризик можна за посиланням ; https://sourceforge.net/projects/loic/

Інтерфейс програми наведено на рисунку 3.3.

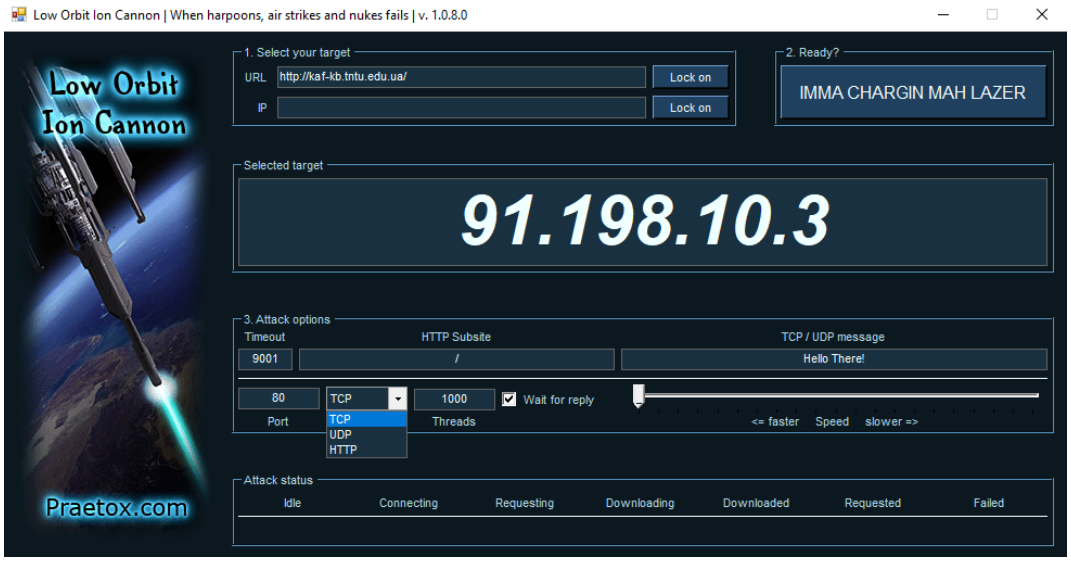

Рисунок 3.3 – Інтерфейс програми LOIC

Як видно на зображені тут все досить інтуїтивно. Є можливість вибрати ціль через IP-адресу чи URL жертви, вибрати на який порт буде відбуватись атака та протокол та додати щось від себе коротким повідомленням.

По звичайній та найвикористовуванішій схемі проводиться атака через 80 порт. Після того як всі функції налаштовано, програма запускається.

Як результат, сторінка не відповідає. Браузер не бачить сторінки, проте дана програма виявилась досить повільною в плані роботи. Результат наведено на рисунку 3.4.

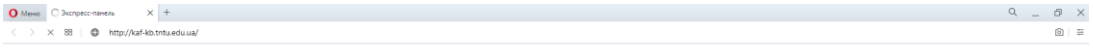

Рисунок 3.4 – Результат DDoS атаки через програму LOIC

Для наступної атаки буде використовуватись програма Fastream Web Stress Test.

Fastream Web Stress Test програма-тестер для перевірки витривалості веб-ресурсу. Дуже легка в використанні та швидка в дії. Особливість програми – мале використання ресурсів комп'ютеру. Інтерфейс програми наведений на рисунку 3.5.

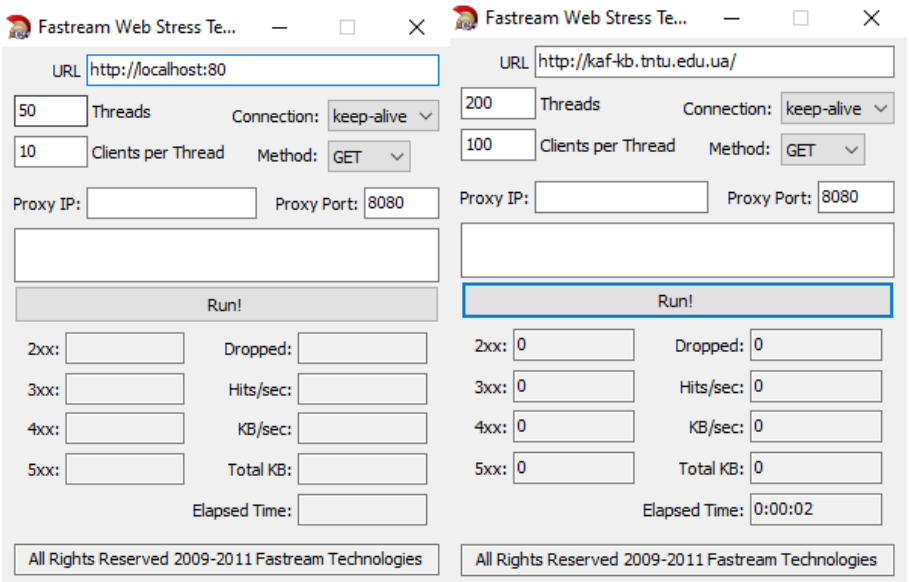

Рисунок 3.5 – Інтерфейс програми Fastream Web Stress Test

В результаті – повна відмова сервера на сайтах. Результат атаки наведено на рисунку 3.6

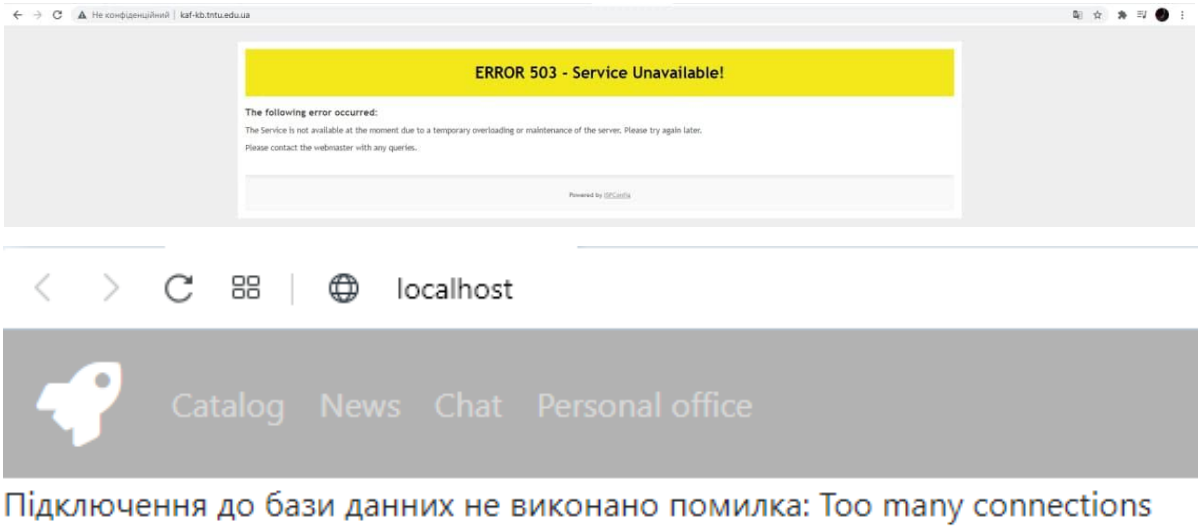

Рисунок 3.6 – Результат DDoS-атаки через програму Fastream Web Stress Test

Дані методи атак вибрані та проведені не дарма.

Простота та доступність – головні критерії при виборі та реалізації атак для нескладних сайтів. Для масивних серверів чи сайтів потрібні більш серйозні методи наведені в перших двох розділах.

3.2 Розробка захисту від DDoS атак

Основні правила для захисту веб-ресурсів від атак зловмисників.

1. Нарощування обчислювальної потужності.Потужний сервер більш витривалий та дає більшу надійність якщо запитів не так багато та DDoS атака не э дыйсно серйозною.

2. Знешкодження вразливостей. Відразу після відбиття атаки потрібно знайти та усунути всі помилки та уразливі місця системи.

3. Відмова від Apache. Apache дуже важко віддає файли і на фундаментальному рівні вразливий до атаки Slowloris яка дозволяє «покласти» сервер навіть з телефону. Користувачі Apache для захисту від атаки створили патч antislowloris.diff.

4. Модуль testcookie. Модуль може захистити від простих атак. Використовується для швидкої перевірки під час DDoS атаки дозволяючи відсіювати непотрібні запити.

5. Зменшення зон, доступних для атаки. Захист націлений на зменшення зон для атаки. Метод обмежує можливості злодіїв для атаки і забезпечує можливість створення центрального захисту.

6. Захист за допомогою Cisco Firepower NG Firewall. Cisco Firepower NG Firewall – адміністративний центр для продуктів Cisco, які використовуються на різних платформах. Забезпечує управління міжмережевими екранами, запобіганням вторгнень, фільтрацією адрес та захистом від шкідливого програмного забезпечення. Центр управління надає зручні у використанні екрани для контролю доступа та захисту. Ця система інтегрується з захистом від удосконаленого шкідливого забезпечення а також надаж інструменти для відстежування по всій мережі. Система дає можливість гнучко налаштовувати аналіз трафіку, який проходить через сенсор Firepower Threat Defence. На рисунку 3.7 зображені потоки даних які обробляються.

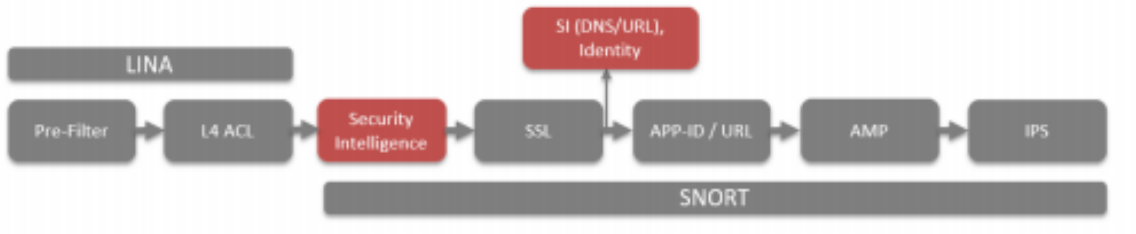

Рисунок 3.7 – Проходження пакетів у Cisco Firepower NG Firewall

7. Професійний захист. Можна старатись та довго прописувати захист, проте в теперішній час є вже готові компанії які пропонують професійний захист від атак будь якого рівня. Тому завжди краще звернутись до професіоналів ніж надіятись на власні знання.

Додаткові рекомендації для уникнення вразливостей:

- Інтернет- провайдери ніколи не повинні дозволяти виконувати підміну адреси у їх мережі. Підміна IP адреси – зародження проблеми.

- Інтернет-провайдери повинні дозволяти клієнтам використовувати BGP flowspec для обмеження вхідного трафіку, щоб зменшити перевантаження під час великих атак.

- Розмобники повинні думати про безпеку при створенні веб-ресурсів.

- Провайдери повинні зберігати історію потоку данних. Ці данні необхідні для визначення джерела атаки та пошуку злодія. Для відстеження атаки достатньо зберігати 1 пакет із 100 тисяч, при цьому зберігаючи конфіденційність підключень клієнтів.

- Адміністратори повинні правильно налаштовувати міжмережевий екран і дозволяти доступ до послуг для тих ,хто потребує а не для всіх.

- Великим плюсом буде можливість дистанційного ребуту мережі(перезапуску) та наявності другого адміністративного чи мережевого інтерфейсу через який можна отримати доступ до сервера основного каналу.

3.3 Програмна реалізація

Принцип дії запропонованого методу повинен захистити від атак за допомогтою масивів обробки вхідних змінних $argc та $argv, написаний на PHP. Для його використання вимагається ОС Linux, тому що в ній влаштований гнучкий і надійний фаєрвол iptables. Принцип дії захисту – блокування IP-адреси, частоти звернення. Передбачається, що на сервері встановлений і працює фаєрвол iptables. Захист вбудовується в php-код сторінок сайту і використовує таблицю MySQL для зберігання тимчасових даних.

Створюється таблиця access_log. Для неї потрібні тільки два поля, для зберігання IP адреси і часу доступу:

```
CREATE TABLE `access_log` (
   `ip` varchar(15) NOT NULL default '',
   `enter_time` int(11) NOT NULL default '0'
) ENGINE=HEAP;
```

Тепер записується функція для виявлення активних IP адрес:

```
function check_ddos(){
    $rec_limit = 4; // Величина выборки
    $time_limit = 1; // Минимальный допустимый промежуток времени между первой и последней записью в выборке
    $ip = $_SERVER['REMOTE_ADDR'];
    // Соединение с БД:
    if (!$db_connection = mysql_pconnect('localhost', 'root', '')){
        die();
    }else{
        if(!mysql_select_db('ddos_test', $db_connection)){
            die();
        }
    }
    mysql_query('DELETE FROM access_log WHERE enter_time < '.(time() - ($time_limit * 2)), $db_connection);
    mysql_query('INSERT INTO access_log (ip, enter_time) VALUES ('".$ip."', '.time().')', $db_connection);
    if ($result = mysql_query('SELECT enter_time FROM access_log WHERE ip='".$ip."' ORDER BY enter_time DESC LIMIT '.$rec_limit)){
        while($row = mysql_fetch_row($result)){
            $result_array[] = $row;
        }
    }
    $rec_count = count($result_array);
    if ($rec_count == $rec_limit){
        $first_time = $result_array[$rec_count - 1][0];
        $last_time = $result_array[0][0];
        if (($last_time - $first_time) < $time_limit){
            iptables_ban_ip($ip);
            exit();
        }
    }
}
```

Все, що робить ця функція – при кожному зверненні до захищеної сторінки сайту пише в таблицю час звернення і IP-адресу клієнта. При цьому кодного разу робиться вибірка з $rec_limit останніх звернень з даної адреси і якщо час від першим і останнім зверненням в цій вибірці має менше значення перемінної $time_limit – викликається функція iptables_ban_ip і даний IP блокується фаєрволом. Сама таблиця тимчасових даних постійно очищується від лишніх даних і містить лише останнє звернення.

Функція для запису особливо нав’язливих IP-адрес в блек-лист фаєрволу:

```
function iptables_ban_ip($ip){
   $command = 'sudo iptables -A INPUT -s '.$ip.' -j DROP';
   system($command);}
```

Залишилось вставити виклик захисту в index.php:

```
check_ddos();
```

Як результат – надійний захист від загроз нескладного типу. Сайт працює. Від серйозних DDoS атак цей захист не допоможе, проте з легкими атаками справиться «на ура».

Висновок до розділу

В даному розділі було проведено атаки різних типів на відмову обслуговування для наведення прикладу та оцінки стану безпеки. Також наведені варіанти захисту веб-ресурсів від DDoS атак на основі найкращих варіантів.

Наведені методи захисту підійдуть для будь якого веб-ресурсу, не є складними для використання чи недоступними для користувача. Зібрані варіанти не потребують великих знань чи зусиль.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ХОРОНИ ПРАЦІ

4.1 Значення адаптації в трудовому процесі

Праця людини безпосередньо пов'язана із виробничим середовищем. Працівник може нормально здійснювати трудову діяльність лише тоді, коли умови зовнішнього середовища відповідають оптимальним. Якщо вони змінюються, стають несприятливими, то на протидію їм організм людини включає спеціальний механізм, який зберігає постійність внутрішнього середовища, або змінює його в межах допустимого. Такий механізм називається адаптацією. Адаптація є важливим засобом попередження травмування, виникнення нещасних випадків у трудовому процесі і відіграє значну роль в охороні праці.

Професійна адаптація — адаптація (пристосування) людини до нових для нього умов праці. Різновид професійної адаптації — виробнича адаптація (пристосування до умов, вимог, норм тощо конкретного виробництва, виробничого процесу).

Адаптація особистості до об'єктивних умов і вимог діяльності забезпечується такими методами: — вдосконалення або зміна в певних межах окремих властивостей; — формування стереотипів дій при незмінних особистісних якостях; — позитивна мотивація до праці; — вироблення індивідуального стилю діяльності. Ці методи, як правило, стосуються тих професій, які ставлять до людини відносні вимоги професійної придатності.

Суть механізму адаптації полягає у змінах меж чутливості аналізаторів, розширенні діапазону фізіологічних резервів організму та зміні в певних межах параметрів фізіологічних функцій. Завдяки фізіологічній адаптації фізичні та біохімічні параметри, які визначають життєдіяльність організму, змінюються у вузьких межах порівняно із значними змінами зовнішніх умов: підвищується стійкість організму до холоду, тепла, недостачі кисню, змін барометричного тиску та інших факторів. Велике значення у фізіологічній адаптації має реактивність організму, його початковий функціональний стан, в залежності від

якого змінюються і відповідні реакції організму на різні дії. Процес фізіологічної адаптації до незвичайних, екстремальних умов проходить декілька стадій, або фаз: спочатку переважають явища декомпенсації (порушення функцій), потім неповного пристосування (активний пошук організмом стійких станів, що відповідають новим умовам середовища) і, нарешті, фаза відносного стійкого пристосування.

Адаптація в трудовій діяльності поділяється на:

Фізіологічна адаптація - це сукупність фізіологічних реакцій, які є в основі пристосування організму до змін оточуючого середовища і направлені на збереження відносної постійності його внутрішнього середовища. Суть механізму адаптації полягає у змінах меж чутливості аналізаторів, розширенні діапазону фізіологічних резервів організму та зміні в певних межах параметрів фізіологічних функцій (підвищується стійкість організму до холоду, тепла, недостачі кисню, змін барометричного тиску).

Психічна адаптація - це процес встановлення оптимальної відповідності особистості до оточуючого середовища в процесі діяльності. Психічна адаптація в процесі праці залежить від психічних властивостей працівника, його психічного стану, психологічних реакцій на стреси, що виникають на роботі, кваліфікації та культури людини, особливостей професійної діяльності, конкурентних умов праці.

Соціальна адаптація - це пристосування працюючої людини до системи відносин у робочому колективі з його нормами, правилами, традиціями, ціннісними орієнтаціями. При несприятливому протіканні соціальної адаптації підвищується рівень стресу на роботі, наслідки якого позначаються на поведінці працівника та можуть призвести до між особових конфліктів, нещасних випадків.

Професійна адаптація - це адаптація до трудової діяльності з усіма її складовими і адаптація до робочого місця, знарядь та засобів праці, об'єктів та предметів праці, особливостей технологічного процесу, головних параметрів роботи. Професійна адаптація виражається у розвитку стійкого позитивного

ставлення працівника до своєї професії, певного рівня оволодіння ним специфічними навичками та уміннями у формуванні необхідних для якісного виконання роботи властивостей.

Кожен із розглянутих видів адаптації впливає на працездатність та здоров'я працівника, формує у нього певний рівень чутливості та стійкості до психоемоційних перевантажень, внаслідок розвитку яких може істотно змінитися надійність професійної діяльності.

4.2 Заходи щодо захисту установки від короткого замикання

Коротке замикання (КЗ) виникає як наслідок неправильного з'єднання в електричному колі через помилкові або злочинні дії людини, дії природних чинників (в тому числі погоди, старіння матеріалів, корозії) або порушення ізоляції частин обладнання, що проводять струм, і зовнішніх механічних пошкоджень в електричних дротах, монтажних дротах, обмотках двигунів і апаратів.

Ізоляція елементів, що проводять струм, може пошкоджуватися під дією високої температури або полум'я (вогню), інфрачервоного випромінювання, переходу напруги з первинної обмотки силового трансформатора на вторинну, за підвищених режимів навантаження (нагрів до високих температур, і як наслідок під час охолодження, конденсується вода).

Час проходження струму короткого замикання не перевищує декількох секунд або навіть долі секунди і залежить від дії апаратів захисту (плавких запобіжників, автоматичних вимикачів).

Струми короткого замикання викликають термічну і електродинамічну дію і супроводжуються різким зниженням напруги в електромережі. Струми короткого замикання можуть перегріти частини, що проводять струм і розплавити дроти (температура до 20 000°С). В результаті виникає частковий або повний розлад електропостачання споживачів.

Електробезпека – це система організаційних і технічних заходів, що забезпечують захист людей від небезпечної і шкідливої дії електричного струму, електричної дуги, електромагнітного поля, статичної електрики.

Основними заходами захисту від ураження електричним струмом є:

- забезпечення недоступності струмопровідних частин для випадкового дотику;
- застосування електроенергії з безпечними величинами напруги;
- усунення небезпеки ураження людей струмом у разі появи напруги на частинах конструкцій електроустаткування;
- застосування індивідуальних захисних засобів від ураження електричним струмом.

Недоступність струмопровідних частин для випадкового дотику досягається ізоляцією їх струмонепровідними матеріалами. Провідники електричного струму повинні мати робочу ізоляцію. Передбачено застосування в деяких випадках додаткової, підсиленої чи лінійної ізоляції.

Застосування малих напруг – дуже ефективний захист від ураження електричним струмом. Для живлення кіл управління технологічним обладнанням, встановленим в особливо небезпечних приміщеннях і приміщеннях з підвищеною небезпекою; кіл управління пересувного устаткування і для живлення ручного інструменту використовують напругу не вище 42 В.

Захисне заземлення, занулення і відключення – основні заходи захисту людей від ураження електричним струмом у разі появи напруги на частинах конструкцій електроустаткування.

Дотик до незахищеного корпусу, який виявився під напругою, рівнозначний однофазному ввімкненню людини в електричну мережу.

Заземлюючим пристроєм називається сукупність заземлювачів – металевих провідників, які з’єднані з землею, і заземлюючих провідників, які з’єднують заземлювані частини електроустаткування з заземлювачами.

Заземлювачі бувають штучні та природні.

Як штучні заземлювачі використовують стальні стрижні, які забивають в ґрунт вертикально і з'єднують між собою стальною шиною зварюванням.

Як природні:

- прокладений у землі водопровід;
- арматуру залізобетонних конструкцій будівель і споруд, яка має з'єднання з землею;
- свинцеві оболонки кабелів, прокладених у землі.

Розрізняють заземлюючі пристрої:

- контурні (заземлення знаходиться у безпосередній близькості від електроустаткування);
- виносні (заземлення розміщені на спеціально виділеній ділянці території підприємства).

Для заземлення електроустаткування у виробничих та інших приміщеннях використовують здебільшого виносні заземлюючі пристрої з штучними заземлювачами. При цьому металеві елементи кожного електрообладнання під'єднують окремими заземлюючими пристроями до транзитної шини, яка прокладається всередині будівлі і не менше, ніж у двох місцях під'єднується до заземлювачів.

У вибухонебезпечних зонах заземлюють електричні машини і апарати, незалежно від величини напруги.

Занулення – свідоме електричне з'єднання з нульовим захисним провідником металевих струмонепровідних частин, які можуть виявитися під напругою.

У електричних мережах розрізняють нульовий захисний ($N_З$) і нульовий робочий ($N_Р$) провідники. Нульовий захисний провідник служить для з'єднання занулюваних частин устаткування з глухо заземленою нейтраллю джерела струму; нульовий робочий провідник – для підключення до основної мережі напругою 380 В освітлювальних приладів, машин і електроапаратів, які працюють за фазової напруги (220 В).

Як нульовий захисний провідник можна використовувати стальні смуги, алюмінієві оболонки кабелів, звичайні проводи. Згідно з галузевими правилами, не допускається використовувати як нульовий захисний провідник нульові робочі провідники.

В електричних мережах з нульовим проводом електроустаткування можна занулювати, заземлювати чи одночасно занулювати і заземлювати. На підприємствах не допускається одне електроустаткування тільки занулювати, інше тільки заземлювати.

Заземлення чи занулення пересувних (переносних) машин і апаратів здійснюється за допомогою спеціального провідника електричного кабеля. В кабелях, які живлять переносні електроприймачі однофазного струму (касові апарати, електронні ваги тощо), крім фазного і нульового робочого провідника, наявний заземлюючий чи нульовий захисний провідник.

Захисне вимкнення – швидкодійний захист, що забезпечує автоматичне відключення електроустаткування, коли в ньому виникає небезпека ураження струмом. Така небезпека може виникнути у випадку:

- замикання фази на корпус електроустаткування,
- пониження опору ізоляції фаз відносно землі,
- появи в мережі більш високої напруги,
- торкання людини до струмопровідних частин.

У цих випадках у мережі змінюються деякі електричні параметри (напруга, струм, опір), що може бути імпульсом, який викликає спрацьовування захисту – відключення пристрою. Принципову схему захисного вимкнення наведено на рисунку.

ВИСНОВКИ

В даній КРБ було розглянуто:

- Методи захисту від DDoS атак
- Основні положення про напади на веб-ресурси, їх типи та методи.
- Причини атак.
- Статистика проведення навмисної шкоди на веб-ресурси компаній та підприємств.
- Аналітика та атака на сайти за допомогою різних методів.
- Рекомендація щодо захисту веб-ресурсів та написаний стартовий метод для уникнення нескладних атак.

Перед завершенням КРБ можна зробити висновок.

Безпека веб-ресурсів невід’ємна частина безпечного життя користувача а також цілісності та працездатності ресурсів компаній та підприємств.

Щодня здійснюють численні атаки від яких страждають люди, саме тому обов’язок спеціалістів по кібербезпеці – захистити та уникнути витіку інформації.

Якщо підсумувати усе вище написане можна чітко зрозуміти, що потрібно серйозно ставитись до створення проекту чи ведення свого веб-ресурсу, шукати нові способи захисту від атак або звернутись до професіоналів.

.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. AWS Amazon [Електронний ресурс] - Режим доступу до ресурсу: https://aws.amazon.com/ru/shield/ddos-attack-protection/ - Дата доступу: 20.05.2021
2. Anti-Malvare [Електронний ресурс] – Режим доступу до ресурсу: https://www.anti-malware.ru/threats/websites-attacks - Дата доступу: 22.05.2021
3. Medium Svyatoslav Login [Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/@svyatoslavlogyn/%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D1%80%D1%8F%D0%B5%D0%BC-%D1%81%D0%B2%D0%BE%D0%B9-%D0%BF%D1%80%D0%BE%D0%B5%D0%BA%D1%82-%D0%BD%D0%B0-%D1%83%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D1%8C-%D0%BA-ddos-e3e5515a7ce9 - Дата доступу 22.05.2021
4. Студопедия.Орг [Електронний ресурс] - режим доступу до ресурсу: https://studopedia.org/9-62702.html - Дата доступу: 24.05.2021
5. Web-LightHouse [Електронний ресурс] - режим доступу до ресурсу: https://web-lighthouse.com/news/типи-сайтів-частина-3-інтернет-магазин/ - Дата доступу: 24.05.2021
6. Wikipedia [електронний ресурс] - Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0 - Дата доступу: 24.05.2021

Додатки

Додаток А – Лістинг файлу functions.php

```
function check_ddos(){
   $rec_limit = 4; // Величина вибірки
   $time_limit = 1; // Мінімально доступний час між першим і останнім запитом
   $ip = $_SERVER['REMOTE_ADDR'];
   // звязок з бд:
   if (!$db_connection = mysql_pconnect('localhost', 'root', 'root')){
      die();    }else{
      if(!mysql_select_db('darkspace', $db_connection)){ die();}    }
   mysql_query('DELETE FROM access_log WHERE enter_time < '.(time() -
($time_limit * 2)), $db_connection);
   mysql_query('INSERT INTO access_log (ip, enter_time) VALUES ("'.$ip.'",
'.time().')', $db_connection);
   if ($result = mysql_query('SELECT enter_time FROM access_log WHERE
ip="'.$ip.'" ORDER BY enter_time DESC LIMIT '.$rec_limit)){
      while($row = mysql_fetch_row($result)){
         $result_array[] = $row;}    }
   $rec_count = count($result_array);
   if ($rec_count == $rec_limit){
      $first_time = $result_array[$rec_count - 1][0];
      $last_time = $result_array[0][0];
      if (($last_time - $first_time) < $time_limit){
         iptables_ban_ip($ip);
         exit();}    }    }
function iptables_ban_ip($ip){
   $command = 'sudo iptables -A INPUT -s '.$ip.' -j DROP';
   system($command);
   iptables -D INPUT -s здесь_IP_адрес -j DROP }
```