slow-ban script

МЕТОД ЗАХИСТУ МЕРЕЖІ ВІД АТАК ДОСТУПУ

ЗМІСТ

ВСТУП

У сучасному глобальному світі мережева безпека має вирішальне значення. Підприємствам необхідно забезпечувати безпечний доступ для співробітників до мережевих ресурсів в будь-який час, для чого сучасна стратегія забезпечення мережевої безпеки повинна враховувати ряд таких факторів, як збільшення надійності мережі, ефективне управління безпекою та захист від постійно еволюціонуючих загроз і нових методів атак. Тому, ця робота присвячена одному з важливих напрямків розробці методу для захисту концепції fail2ban від блокування доступу дозволеним користувачам.

Концепція Fail2Ban полягає у відмові пакетам з певної IP-адреси зловмисника на певний час, і зловмисник (хакер) з цієї IP-адреси більше не може отримати доступ до сервера.

Fail2ban буде блокувати весь трафік користувачів, які перебувають позаду NAT мережі (використовувати одну загальнодоступну IP-адресу). Тобто якщо користувач позаду NAT буде заблокований, разом з ним будуть заблоковані всі інші користувачі. Але якщо сервер буде налаштований за розробленим методом, він все одно може бути дуже захищений, надавши доступ для дозволених користувачів з будь-якої IP-адреси. Для розуміння рівня захисту серверу після налаштування далі будуть розрахунки оцінки ефективності розробленого методу.

1. ВАЖЛИВІСТЬ КІБЕРБЕЗПЕКИ В СУЧАСНИХ МЕРЕЖАХ ТА СИСТЕМАХ

На сьогодні кібератаки дуже розповсюджені, нещодавні звіти показують, що хакери атакують комп'ютери у всьому світі кожні 39 секунд. Кібератака – це шкідлива, здійснювана свідомо спроба людини або організації проникнути в інформаційну систему іншої людини або організації. Як правило, порушуючи роботу мережі жертви, хакер прагне отримати вигоду.

Зловмисники прагнуть користуватися вразливістю корпоративних систем, що обумовлює щорічне зростання кіберзлочинності. Часто хакери вимагають викуп: 53% кібератак призвели до збитків у розмірі 500 000 дол. США або більше. Кібератаки також можуть мати приховані мотиви. Деякі спроби хакерів знищити системи і дані є своєрідними проявами «хактівізма».

Ботнет – це мережа пристроїв, заражених шкідливим програмним забезпеченням, наприклад вірусами. Хакери можуть управляти ботнетом як єдиної групою без відома власників з метою збільшення масштабу атак. Найчастіше ботнети використовуються для створення непідйомною навантаження на системи в результаті DDoS-атак.

Поширені типи кібератак [1]:

1. **Шкідливе ПО.** Термін «шкідливе ПО» вживається, коли мова йде про шпигунському ПЗ, програмах-здирників, віруси і інтернет-хробаків. Шкідливе ПО проникає в мережу через вразливість, як правило, коли користувач переходить по небезпечній посиланням або відкриває вкладення в електронній пошті, що призводить до встановлення такого ПО. Опинившись всередині системи, шкідливе ПЗ може:

– блокувати доступ до ключових компонентів мережі (віруси-вимагачі);

– встановлювати шкідливі програми або додаткове шкідливе ПЗ;

– приховано збирати дані з жорсткого диска і відправляти їх зловмисникові (шпигунське ПЗ);

– порушувати роботу деяких компонентів і виводити систему з ладу.

2. Фішинг – це розсилка, як правило, по електронній пошті, шахрайських повідомлень, які виглядають так, ніби вони відправлені надійним адресатом. Метою цієї діяльності є крадіжка конфіденційних даних, наприклад про кредитні картки або облікових записах, або встановлення зловмисного програмного забезпечення на комп'ютері жертви. Фішинг стає все більш поширеною кіберзагроз.

3. Атаки через посередника (Man-in-the-Middle, MitM) виникають, коли хакери впроваджуються у взаємодію двох сторін. Отримавши доступ до трафіку, хакери можуть фільтрувати і красти дані.

Два найпоширеніші способи здійснення атак через посередника:

1). У незахищеною загальнодоступною мережі Wi-Fi хакери можуть перехопити контроль на ділянці між пристроєм відвідувача і мережею. Не знаючи про це, відвідувач буде передавати всі дані через хакера.

2). Коли шкідливе ПО проникає на пристрій, хакер може встановити додатки для аналізу всіх даних жертви.

4. Атака типу «відмова в обслуговуванні» (Denial of Service, DoS) переповнює системи, сервери або мережі трафіком, що призводить до вичерпання ресурсів і пропускної здатності. В результаті система втрачає здатність виконувати нормальні запити. Хакери також можуть використовувати скомпрометовані пристрої для організації атак. Це називається розподіленою атакою типу «відмова в обслуговуванні» (Distributed Denial of Service, DDoS-атака).

5. SQL ін'єкція – це передача шкідливого SQL-коду на сервер, що обробляє SQL-запити, в результаті чого сервер розкриває дані, що не

передбачалося розкривати. Щоб впровадити SQL-код, іноді досить ввести шкідливий код в поле пошуку уразливого веб-сайту.

6. Експлойт нульового дня виникає після розкриття уразливості мережі і до створення виправлення або вирішення цієї проблеми. У цей часовий інтервал хакери атакують з використанням відкритої уразливості. Для виявлення загроз, пов'язаних з уразливістю нульового дня, потрібен постійний моніторинг.

7. Тунелювання DNS – це використання протоколу DNS для передачі трафіку, який не належить до DNS, через порт 53. Ця атака дозволяє відправляти через DNS трафік HTTP та інших протоколів. Тунелювання DNS може використовуватися в різних правомірних цілях. Однак існує можливість використовувати служби VPN для тунелювання DNS зі злим умислом. З їх допомогою під виглядом трафіку DNS можна передавати дані, які зазвичай передаються по інтернет-каналу. За допомогою DNS-запитів зловмисник може отримати дані з скомпрометованої системи і перенести їх в своє середовище. Їх також можна використовувати для спрямування керуючих зворотних викликів з інфраструктури хакера в скомпрометовану систему.

Деякі організації опублікували **рекомендації щодо передових практик безпеки**:

– **Оцінка ризиків** – Розуміння цінності того, що ви захищаєте, допоможе вам виправдати витрати на безпеку.

– **Створення політики безпеки** – Розробіть політику, яка чітко окреслює корпоративні правила, обов'язки та очікування.

– **Заходи фізичної безпеки** – Обмежте доступ до комунікаційних шаф, серверних кімнат, а також забезпечте дотримання норм протипожеженої безпеки.

– **Ретельна перевірка персоналу** – При прийомі на роботу необхідно належним чином вивчати анкетні дані та минуле співробітників.

– **Створення і перевірка резервних копій** – Регулярно виконуйте резервне копіювання та перевіряйте можливість відновлення даних з них.

– **Підтримка виправлень і оновлень системи безпеки** – Регулярно оновлюйте операційні системи і програмне забезпечення серверів, клієнтів і мережних пристроїв.

– **Використання засобів контролю доступу** – Налаштуйте ролі і рівні привілеїв користувачів, а також надійну аутентифікацію.

– **Регулярна перевірка реагування на інциденти** – Сформуйте команду реагування на інциденти і випробовуйте сценарії реагування на надзвичайні ситуації.

– **Впровадження інструменту моніторингу, аналізу та керування мережею** – Виберіть рішення для моніторингу безпеки, яке інтегрується з іншими технологіями.

– **Впровадження мережних пристроїв безпеки** – Використовуйте нове покоління маршрутизаторів, міжмережних екранів та інших пристроїв безпеки.

– **Впровадження комплексного рішення для захисту кінцевих вузлів** – Використовуйте корпоративні версії антивірусів та захисних програм від усіх видів шкідливого ПЗ.

– **Навчання користувачів** – Навчайте користувачів та співробітників процедурам безпеки.

– **Шифрування даних** – Шифруйте всі конфіденційні дані компанії, включно з електронною поштою.

Очевидно, що інструментів для забезпечення безпеки дуже багато, що призводить до нових проблем типу узгодженості їх сумісної роботи та вибору оптимального комплексу інструментів для конкретної організації. Також внутрішні недоліки окремих технологій потрібно враховувати при розробці комплексу заходів захисту.

2. ВИКОРИСТАННЯ FAIL2BAN ДЛЯ ЗАХИСТУ МЕРЕЖІ

В роботі був проведений аналіз існуючих інструментів боротьби з кібератаками та виявлені недоліки деяких з них. В цьому розділі буде розглянутий класичний інструмент Fail2Ban [2, 3], що працює шляхом моніторингу файлів журналів для вибраних записів та запуску сценаріїв на їх основі. Найчастіше це використовується для блокування вибраних IP-адрес, які можуть належати вузлам, які намагаються порушити безпеку системи.

Він може заборонити будь-яку IP-адресу хосту, яка робить занадто багато спроб входу в систему або виконує будь-які інші небажані дії протягом часу, визначеного адміністратором. Включає підтримку як IPv4, так і IPv6. Більший час блокування може бути налаштований для тих, хто постійно повертається.

Зазвичай Fail2Ban встановлюється для заборони заблокованого хоста протягом певного періоду, щоб не "блокувати" будь-які справжні з'єднання, які могли бути тимчасово неправильно налаштовані. Однак, забороненого часу в кілька хвилин зазвичай достатньо, щоб зупинити мережеве з'єднання, заповнене шкідливими з'єднаннями, а також зменшення ймовірності успішної атаки на словники.

Fail2Ban може виконувати кілька дій при виявленні IP-адреси зловмисника: оновлювати правила Netfilter / iptables або PF firewall, таблицю hosts.deny TCP Wrapper, щоб відхилити IP-адресу зловмисника; сповіщення електронною поштою; або будь-яка визначем дія, яку може виконувати скрипт Python.

Стандартна конфігурація постачається з фільтрами для Apache, Lighttpd, sshd, vsftpd, qmail, Postfix та Courier Mail Server. Фільтри визначаються регулярними виразами Python, які можуть бути зручно налаштовані адміністратором, знайомим із регулярними виразами.

Поєднання фільтра та дії відоме як "jail" (таблиця заборонених адрес) і є причиною того, що шкідливий хост не може отримати доступ до певних мережевих служб. Окрім прикладів, що розповсюджуються разом із

програмним забезпеченням, для будь-якого процесу, що стикається з мережею, який створює файл журналу доступу, може бути створена "jail".

Далі показано що fail2ban може робити протягом 2 днів на щойно створених серверах без будь-яких програм та з базовим цифровим захистом.

Сервер у Bangalore

Всього невдалих спроб-- 475

Всього заблоковано -- 99

Fig. 1. Статистика серверу у Bangalore на протязі 2 днів

Сервер у New York

Всього невдалих спроб -- 4313

Всього заблоковано -- 814

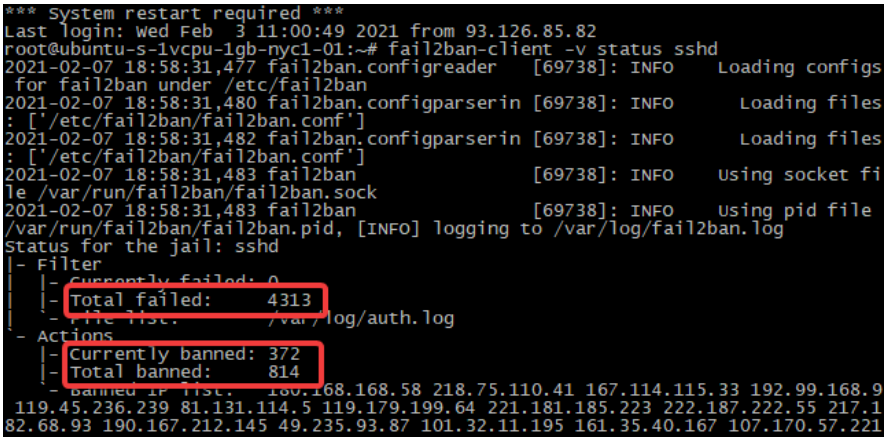


Fig. 2. Статистика серверу у New York на протязі 2 днів

Сервер у Frankfurt

Всього невдалих спроб -- 3712

Всього заблоковано -- 875

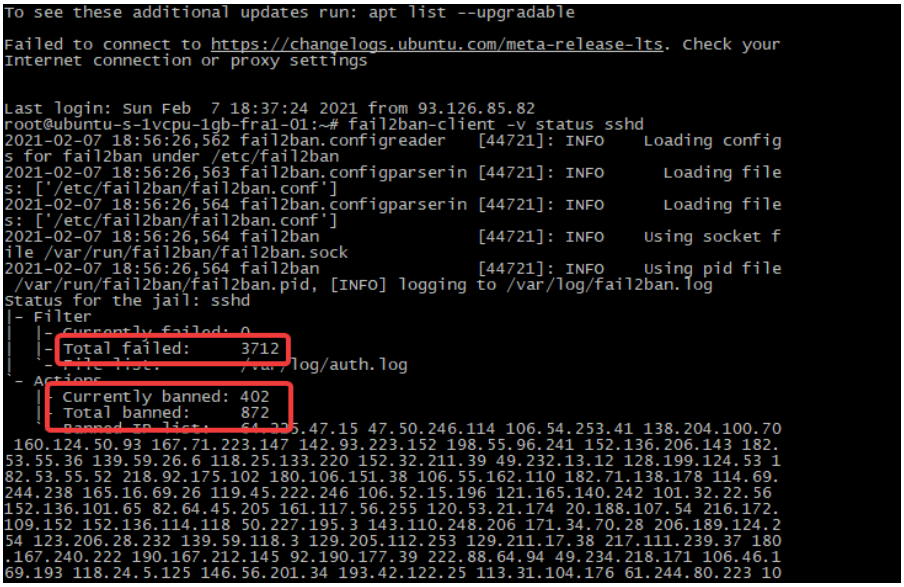


Fig. 3. Статистика серверу у Frankfurt на протязі 2 днів

Сервер у Singapore

Всього невдалих спроб -- 3942

Всього заблоковано -- 728

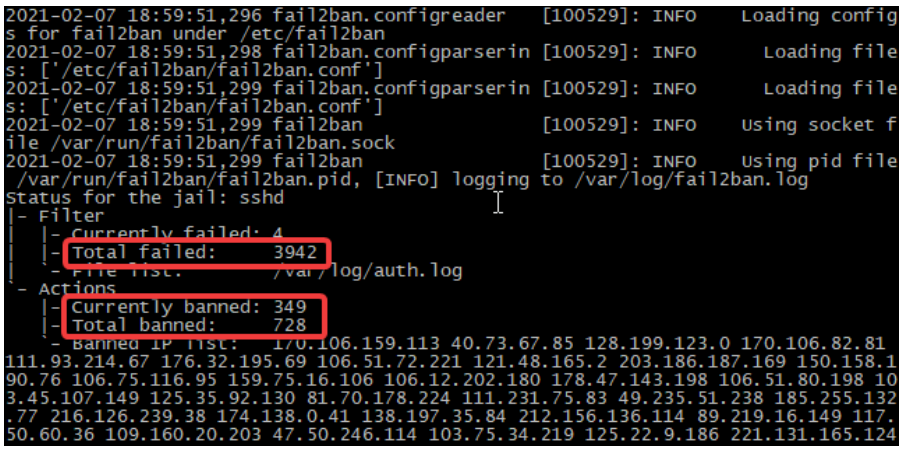


Fig. 4. Статистика серверу у Singapore на протязі 2 днів

3. РОЗРОБКА МЕТОДУ ЗАХИСТУ МЕРЕЖІ ВІД АТАК ДОСТУПУ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ FAIL2BAN

Fail2Ban забороняє IP-адресу протягом часу, заданого адміністратором і людина з цієї IP-адреси більше не може отримати доступ до сервера. Тобто якщо хтось з NAT мережі спробує згадати пароль на протязі кількості спроб, які адміністратор налаштує, наприклад, з великого офісу організації, всі інші люди в цьому офісі втратять доступ до цього сервера.

Але якщо сервер буде налаштовано за допомогою власних сценаріїв fail2ban, він все одно може бути дуже захищений, зберігаючи доступ для дозволених користувачів з будь-якої IP-адреси.

Якщо хакер спробує отримати доступ методами грубого підбору (brute force) паролю сервера, і його спроби не вдаються з поточної IP-адреси, можливо, хакер змінить IP-адресу для перебору. У цьому випадку наші власні сценарії fail2ban також можуть допомогти. Бо можливо хакер не буде змінювати IP-адресу та продовжить проводити повільні спроби [4].

Сценарій fail2ban для обмеження швидкості brute force

Щоб уникнути раніше згаданих проблем, наші скрипти блокують IP-адресу не на деякий час, а сповільнюють швидкість його з'єднання із сервером. Отже, хакер не може застосовувати грубий перебір 100 або 1000 разів на секунду, а лише, наприклад, 1 раз на секунду.

В основну папку дій fail2ban потрібно скопіювати або створити файл .conf з ім'ям, наприклад **slow-ban.conf**.

У цьому файлі буде викликатись інший скрипт. У цьому новому сценарії (наприклад **slow-ban-iptables.sh**) ми додамо правило iptables, яке обмежить вхідну швидкість для конкретної IP-адреси (буде передано як змінна) до 1 пакету в секунду (це число можна змінити в **slow- ban.conf**).

Після цього у конфігурації за замовчуванням fail2ban у конкретному додатку, наприклад у ssh, нам потрібно додати **banaction = slow-ban**, цей рядок повідомляє fail2ban використовувати наш файл slow-ban.conf для заборони з'єднань по ssh. Крім того, буде гарною ідеєю змінити параметри за замовчуванням, такі як кількість спроб на 3 і час дії до декількох днів.

Налаштування

Після встановлення fail2ban скопіювати **slow-ban.conf** та **slow-ban-iptables.sh** скріпти до **/etc/fail2ban/action.d/**

Потім скопіювати конфігураційний файл jail.conf до jail.local чи просто змінювати jail.conf файл у каталозі /etc/fail2ban/ як завгодно, але використовуйте

banaction = slow-ban

slow-ban.conf файл:

[Definition]

actionstart = bash /etc/fail2ban/action.d/slow-ban-iptables.sh start
actionstop = bash /etc/fail2ban/action.d/slow-ban-iptables.sh stop
actioncheck =
actionban = bash /etc/fail2ban/action.d/slow-ban-iptables.sh ban <ip>
actionunban = bash /etc/fail2ban/action.d/slow-ban-iptables.sh unban <ip>

[Init]

```
1
2 [Definition]
3
4 actionstart = bash /etc/fail2ban/action.d/slow-ban-iptables.sh start
5
6 actionstop = bash /etc/fail2ban/action.d/slow-ban-iptables.sh stop
7
8 actioncheck =
9
10 actionban = bash /etc/fail2ban/action.d/slow-ban-iptables.sh ban <ip>
11
12 actionunban = bash /etc/fail2ban/action.d/slow-ban-iptables.sh unban <ip>
13
14 [Init]
```

Fig. 5. slow-ban.conf файл

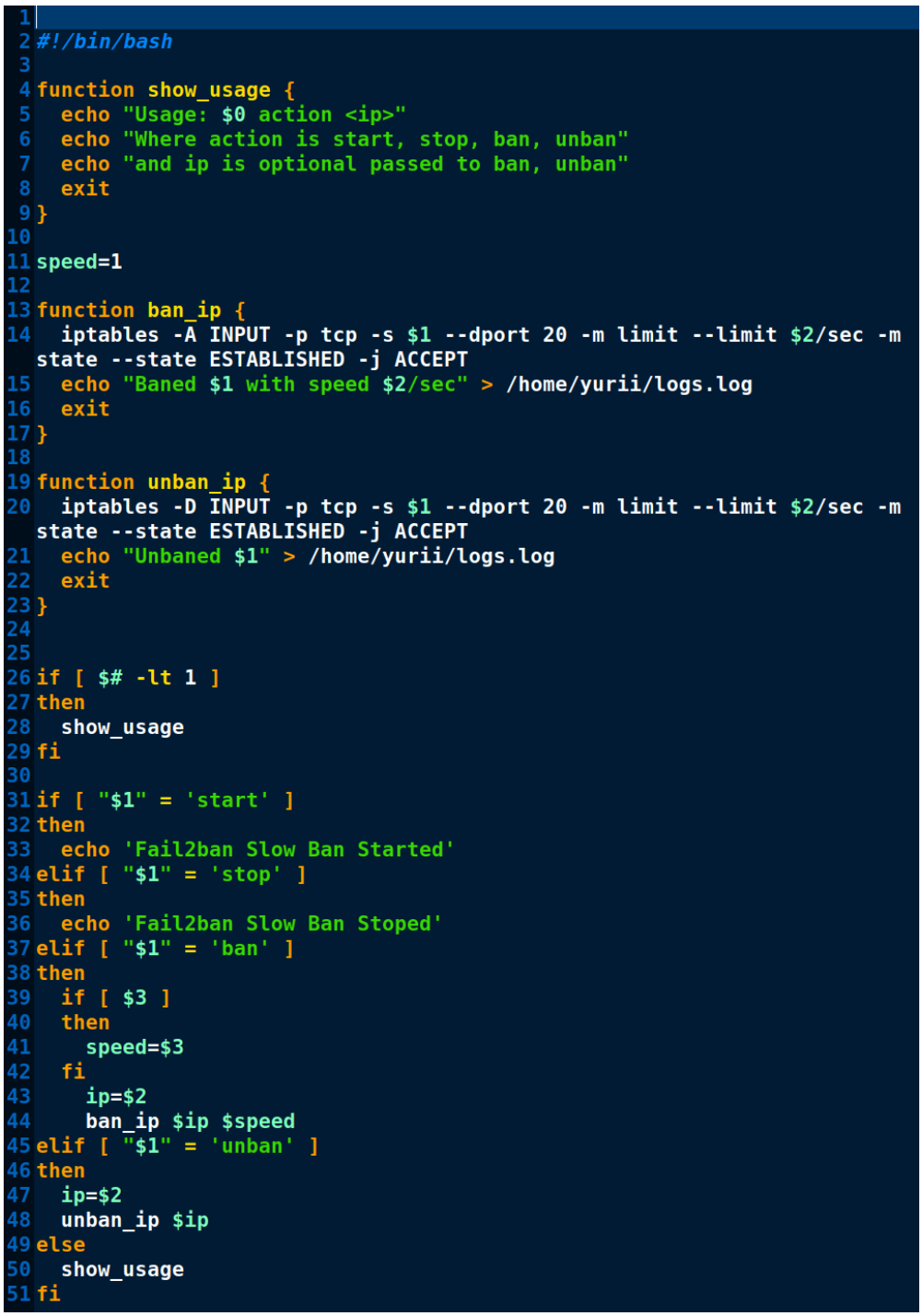
slow-ban-iptables.sh файл:

#!/bin/bash

function show_usage {
  echo "Usage: $0 action <ip>"
  echo "Where action is start, stop, ban, unban"
  echo "and ip is optional passed to ban, unban"
  exit
}

```
speed=1

function ban_ip {
  iptables -A INPUT -p tcp -s $1 --dport 20 -m limit --limit $2/sec -m state --state ESTABLISHED -j ACCEPT
  echo "Baned $1 with speed $2/sec" > /home/yurii/logs.log
  exit
}

function unban_ip {
  iptables -D INPUT -p tcp -s $1 --dport 20 -m limit --limit $2/sec -m state --state ESTABLISHED -j ACCEPT
  echo "Unbaned $1" > /home/yurii/logs.log
  exit
}


if [ $# -lt 1 ]
then
  show_usage
fi

if [ "$1" = 'start' ]
then
  echo 'Fail2ban Slow Ban Started'
elif [ "$1" = 'stop' ]
then
  echo 'Fail2ban Slow Ban Stoped'
elif [ "$1" = 'ban' ]
```

```
then
  if [ $3 ]
  then
    speed=$3
  fi
    ip=$2
    ban_ip $ip $speed
elif [ "$1" = 'unban' ]
then
  ip=$2
  unban_ip $ip
else
  show_usage
fi
```



```
#!/bin/bash

function show_usage {
  echo "Usage: $0 action <ip>"
  echo "Where action is start, stop, ban, unban"
  echo "and ip is optional passed to ban, unban"
  exit
}

speed=1

function ban_ip {
  iptables -A INPUT -p tcp -s $1 --dport 20 -m limit --limit $2/sec -m state --state ESTABLISHED -j ACCEPT
  echo "Baned $1 with speed $2/sec" > /home/yurii/logs.log
  exit
}

function unban_ip {
  iptables -D INPUT -p tcp -s $1 --dport 20 -m limit --limit $2/sec -m state --state ESTABLISHED -j ACCEPT
  echo "Unbaned $1" > /home/yurii/logs.log
  exit
}


if [ $# -lt 1 ]
then
  show_usage
fi

if [ "$1" = 'start' ]
then
  echo 'Fail2ban Slow Ban Started'
elif [ "$1" = 'stop' ]
then
  echo 'Fail2ban Slow Ban Stoped'
elif [ "$1" = 'ban' ]
then
  if [ $3 ]
  then
    speed=$3
  fi
    ip=$2
    ban_ip $ip $speed
elif [ "$1" = 'unban' ]
then
  ip=$2
  unban_ip $ip
else
  show_usage
fi
```

Fig. 6. slow-ban-iptables.sh файл

4.ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНОГО МЕТОДУ

Знаходження безпечного часу використання пароля.

Це час поки зловмисник виконує повний перебір паролів методом грубого підбору (brute force) паролю. Звичайно паролі будуть підбирати із словників можливих паролів. Але ця формула потрібна лише для порівняння можливостей захисту.

$$T = Q * T s$$

Ts - час однієї спроби підбору пароля

Q - всі можливі комбінації символів

$$Q = A^s$$

A - кількість можливих символів у паролі

S - кількість символів з якої складається пароль

A = 95 символів

Якщо система захищена 6-значним паролем(та зловмисник знає про це), без fail2ban slow-ban (наприклад, швидкість brute force 100 спроб в секунду) тоді це буде:

$$T = 95^6 * \frac{1}{100} = 7350918906с = 850800днів$$

Якщо система захищена 6-значним паролем(та зловмисник знає про це), з fail2ban slow-ban (швидкість brute force не може перевищувати 1 спробу в секунду) тоді це буде:

$$T = 95^6 * 1 = 735091890625c = 8508007днів$$

Як видно персональний скрипт збільшує час до повного перебору у стільки разів, наскільки швидше зловмисник перебирає пароль без блокування на 1 спробу в секунду.

Більш нагляним буде шанс паролю не бути знайденим протягом певного періоду часу. Наприклад візьмемо 20 днів.

$$P(t) = 1 - Pp(t)$$

Pp(t) - шанс паролю не бути знайденим протягом періоду часу t

$$Pp(t) = \frac{Qn(t)}{Q}$$

Q - всі можливі комбінації символів

$$Qn(t) = \frac{t}{T\,s}$$

T s – час однієї спроби підбору пароля
t – час, що нас цікавить

$$Pp(t) = \frac{t}{T}$$

T – час повного brute force паролю

Наприклад при t = 20 днів шанс розкриття паролю буде:

Якщо система захищена 6-значним паролем(та зловмисник знає про це), без fail2ban slow-ban (наприклад швидкість brute force 100 спроб в секунду) тоді це буде:

$$Pp(t) = \frac{20}{850800} = 0.0000235$$

Якщо система захищена 6-значним паролем(та зловмисник знає про це), з fail2ban slow-ban (швидкість brute force не може перевищувати 1 спробу в секунду) тоді це буде:

$$Pp(t) = \frac{20}{8508007} = 0.00000235$$

Та шанс паролю не бути розкритим:

Якщо система захищена 6-значним паролем (та зловмисник знає про це), без fail2ban slow-ban (наприклад швидкість підбору паролю 100 спроб в секунду) тоді це буде:

$$P = 1 - 0.0000235072872591 = 0.9999764$$

Якщо система захищена 6-значним паролем (та зловмисник знає про це), з fail2ban slow-ban (швидкість підбору паролю не може перевищувати 1 спробу в секунду) тоді це буде:

$$P = 1 - 0.0000023507267918 = 0.99999764$$

Як видно персональний скрипт зменшує шанс паролю бути розкритим у стільки разів, наскільки швидше зловмисник перебирає пароль без блокування на 1 спробу в секунду.

Таким чином, сценарій fail2ban для обмеження швидкості спроб brute force дозволяє підключитися до сервера за допомогою SSH, але не блокує весь трафік SSH. Таким чином, він захищає концепцію fail2ban від заборони дозволених користувачів, а також добре захищає сервер. Звичайно, заборона за замовчуванням буде більш безпечною. Але для деяких користувачів або серверів цей скрипт буде дуже корисним. Безпека сервера зростатиме в стільки разів, у скільки 1 пакет в секунду повільніший, ніж швидкість brute force хакера. Також існує ймовірність того, що протягом деякого фіксованого часу пароль буде підібраний в цій роботі був розрахований час для двох випадків - без fail2ban та з персональним скриптом.

ВИСНОВКИ

Проведений аналіз показав стрімке зростання сучасних мережі розвиваються у бік збільшення кількості користувачів та сервісів, які надаються онлайн. Разом з тим, що користувачі (приватні або підприємства і т.п.) все більше зберігають та передають через Інтернет конфіденційної інформації, зростає потреба захисту цих даних від зловмисників. Тому робота присвячена безсумнівно актуальній темі розробки ефективного методу обмеження доступу до системи при збереженні доступності для легітимних користувачів.

В роботі були вирішені наступні завдання:

1. Проведений аналіз існуючих рішень щодо забезпечення безпеки в сучасних мережах та системах.

2. Виявлені проблеми з використанням технологій обмеження доступу методами грубого підбору (brute force), що пов'язані з побічним блокуванням легітимних користувачів.

3. Розроблений та впроваджений метод захисту мережі від атак доступу за допомогою технології fail2ban при зберіганні доступності ресурсів для легітимних користувачів.

4. Розраховано ймовірність події, коли пароль не буде підібраним протягом певного періоду часу, що дає можливість оцінити ефективність розробленого методу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке кібератака [Електронний ресурс] / Режим доступу: https://www.cisco.com/c/ru_ru/products/security/common-cyberattacks.html

2. Офіційний сайт fail2ban [Електронний ресурс] / Режим доступу: https://www.fail2ban.org/wiki/index.php/Main_Page

3. Інформація про наслідки кібератак та необхідність мір [Електронний ресурс] / Режим доступу: https://www.google.com.ua

4. Способи налаштування fail2ban [Електронний ресурс] / Режим доступу: https://putty.org.ru/articles/fail2ban-ssh.html

АНОТАЦІЯ

Актуальність: у зв’язку зі стрімким зростанням проблеми інформаційної безпеки (кількості та якості кібератак) в сучасних мережах та системах гостро стоїть питання розробки та впровадження інструментів забезпечення безпеки. Але треба при цьому організувати гарантований доступ легітимних користувачів, бо побічною дією багатьох технологій є хибне спрацьовування і обмеження доступу легітимних користувачів. Саме тому цій актуальній темі присвячена робота.

Мета: розробка методу захисту мережі від атак доступу за допомогою технології fail2ban при зберіганні доступності ресурсів для легітимних користувачів.

Завдання:

1. Провести аналіз існуючих рішень щодо забезпечення безпеки в сучасних мережах та системах.

2. Виявлення проблем з використанням технологій обмеження доступу методами грубого підбору (brute force), що пов'язані з побічним блокуванням легітимних користувачів.

3. Розробка та впровадження методу захисту мережі від атак доступу за допомогою технології fail2ban при зберіганні доступності ресурсів для легітимних користувачів.

4. Розрахунок ймовірності події, коли пароль не буде підібраним протягом певного періоду часу.

Використана методика дослідження: при дослідженні були використані метод аналізу, методи класифікації, методи натурного експерименту.

Загальна характеристика роботи: робота присвячена актуальній темі забезпечення безпеки доступу до ресурсів за допомогою широко використовуваного інструменту fail2ban. При використанні fail2ban досягнуто не тільки реалізацію концепції fail2ban, але й можливість організації доступу легітимних користувачів.