оснащена двома баками різних модифікацій (бак для палива і бак для відходу під утилізацію).

В нашій розробці ми по-перше максимально ефективно використовуємо тепло робочого тіла завдяки циклу Стірлінга-Карно та ефективного теплового захисту, чого не можливо в інших розробках через використання циклу Отто та повної за відсутності теплового захисту. По-друге ми цілковито відмовилися від нафтових та йому подібних типів енергії, що дуже забруднюють навколишнє середовище.

Отже ми отримуємо перспективний двигун, який може змінити наш уявлення про теплові двигуни і разом з тим вирішити проблеми екології.

Кудярський І.С.
студент,
Науковий керівник: **Вовк Р.Б.**
кандидат технічних наук, доцент,
доцент кафедри програмного забезпечення автоматизованих систем,
Івано-Франківський національний технічний університет нафти і газу

МЕРЕЖЕВІ АТАКИ В ІНТЕРНЕТ СЕРЕДОВИЩІ ТА МЕТОДИ БОРОТЬБИ З НИМИ

З появою мережі Інтернет людське суспільство стає все більш інформаційним. Вона надає нові можливості вільного і швидкого доступу до великого об’єму інформації, здатності оперативно обмінюватися нею. Однак ця технологія приховує загрозу розголошення та втрати важливих корпоративних документів, персональних даних і навіть державних таємниць, а атаки зловмисників, стають дедалі витонченішими та небезпечними. Саме тому мережеву безпеку слід всебічно вивчати, навіть якщо потенційні загрози здаються примарними. В цьому і полягає актуальність вибраної тематики дослідження.

Завдяки широкому застосуванню Інтернету не лише в корпоративних, але й приватних цілях, а також поширенню простих для розуміння середовищ розробки та операційних систем хакери, використовуючи різноманітні атаки, отримують доступ до багатьох ресурсів користувачів. Щоб уявити потенційні загрози безпеки даних або мережі, треба створити чітку класифікацію атак і вивчити методи боротьби з ними. На даний момент більшість існуючих класифікацій не завжди є інформативними та влучними. Тому, в даному дослідженні було наведено класифікацію мережевих атак:

1. Sniffer-атака являє собою прикладну програму, яка перехоплює всі мережеві пакети, що передаються через певний домен. На даний момент сніффери повністю законні і виконують в мережі діагностику несправностей та аналіз трафіку. Деякі мережеві додатки та програми передають дані у текстовому форматі і скориставшись сніффером можна отримати важливу

персональну інформацію (наприклад, логіни, паролі та імена користувачів). Оскільки більшість користувачів використовують однакові паролі для доступу до різних ресурсів, операційних середовищ та мережевих додатків, то сніффінг пакетів є досить небезпечною атакою.

2. IP-спуфінг відбувається тоді, коли хакер видає себе зареєстрованим користувачем, використовуючи IP-адресу з допустимого діапазону дійсних IP-адрес, або авторизовану зовнішню адресу, яка має доступ до певних ресурсів мережі. Зазвичай IP-спуфінг має на меті заміну важливої інформації некоректною, введення шкідливих команд в потік даних, які передаються між клієнтами і сервером. Якщо таблиці маршрутизації будуть змінені злочинцем і він направить трафік на неіснуючу IP-адресу, то йому відкриється доступ до всіх пакетів, внаслідок чого він стає санкціонованим користувачем [1].

3. Віруси та шкідливі програми типу «троянський кінь». Комп'ютери користувачів, підключені до мережі Інтернет, є досить вразливими до вірусів та шкідливих програм типу «троянський кінь». Під вірусом розуміють такий шкідливий програмний продукт, який проникає в комп'ютер жертви або певні програми для здійснення небажаних функцій. Віруси можуть завантажуватися через мережеві канали, але їхня активація відбувається лише внаслідок дій користувача. «Трояни» або «троянські коні» – це повноцінні робочі програми, які видають себе в системі за корисні додатки, але насправді здійснюють шкідливий вплив на неї. Після проникнення в комп'ютер через канали зв'язку «трояни» активуються внаслідок дій користувача або самостійно, використовуючи уразливі місця операційної системи.

4. Парольні атаки. Цей тип мережевих атак можна розглядати як симбіоз усіх попередніх, оскільки зловмисник для отримання паролів жертв може використовувати сніффери пакетів, IP-спуфінг та навіть віруси і шкідливі програми типу «троянський кінь». Однак, досить часто хакери, користуючись методом підбору, намагаються вгадати пароль, тобто якщо злочинець авторизується в системі за допомогою пароля звичайного користувача, то він отримає доступ лише до загальних ресурсів, але якщо він підбере пароль користувача з певними привілеями, то це зможе вплинути на систему вцілому навіть, коли пароль, під яким він проник буде змінений [1].

5. DoS (Denial of Service – відмова в обслуговуванні) – це атака на обчислювальну техніку, для доведення її до відмови, тобто такого стану, коли санкціоновані користувачі не можуть отримати доступ до системних ресурсів, або цей доступ утруднений. На даний час DoS і DDoS-атаки найпопулярніші, бо дозволяють довести до відмови практично будь-яку систему, не залишаючи юридично вагомих доказів зловмисних втручань.

Розглянемо найбільш відомі різновиди цих атак [2]:

5.1 HTTP-флуд і ping-флуд – це найбільш примітивний вид DoS-атаки при якому для атаки на сервер зловмисник надсилає невеликий за об'ємом HTTP-пакет, але такий, щоб сервер відповів на нього пакетом, розміром більшим в декілька сотень раз. Зловмиснику щоразу доводиться змінювати свою IP-адресу

на IP-адреси мережевих вузлів, щоб HTTP-пакети, які надсилаються у відповідь не викликали відмову в обслуговуванні у нього самого.

5.2 Атака Smurf (ICMP-флуд) – один з найнебезпечніших видів DoS-атак, оскільки після неї відмова в обслуговуванні у комп'ютера жертви стається майже завжди. Зловмисник відправляє ping-запит, через широкомовну розсилку для аналізу вузлів, що в реальному часі працюють в системі. За допомогою підсилювальної мережі здійснюється надсилання підробленого ICMP пакету, після чого зловмисник замінює свою адресу адресою жертви і всі вузли присилають її комп'ютеру відповідь на ping-запит хакера.

5.3 Атака Fraggle майже ідентична Smurf-атаці, з тією відмінністю, що замість ICMP пакетів використовуються пакети UDP. Принцип її дії полягає в тому, що широкомовною розсилкою на порт жертви надсилаються echo-команди. Згодом свою IP-адресу хакер підмінює IP-адресою жертви і залежно від числа вузлів в мережі, вона отримує певну кількість повідомлень у відповідь.

5.4 Атака за допомогою переповнення пакетами SYN (SYN-флуд). Принцип дії даної атаки полягає в тому, що хакер, змінивши свою IP-адресу неіснуючою, відправляє із одного комп'ютера до іншого пакет SYN. Комп'ютер, який прийняв надіслані пакети відправляє на неіснуючу IP-адресу SYN/ACK у відповідь та переходить у стан SYN-RECEIVED. Оскільки повідомлення SYN/ACK не знайде потрібного йому комп'ютера, то потенційне з'єднання буде поміщено в чергу, яка завершиться приблизно через одну хвилину. Кібер-злочинці користуються цим і відправляють одразу декілька пакетів з інтервалом в 10-15 секунд, що повністю вичерпує ресурси жертви. В результаті даної атаки визначити джерело досить важко, оскільки хакер постійно змінює IP-адресу.

Для активної і дієвої боротьби з наведеними вище мережевими атаками найчастіше використовуються наступні методи:

1. Криптографія – найбільш дієвий метод подолання мережевих атак. Якщо мережевий канал захищений криптографічним способом, то зловмисник перехоплює не цілісне повідомлення, а зашифрований текст, представлений у вигляді послідовності бітів [3]. Але, якщо злочинець отримає інформацію про криптографічну сесію, тобто ключ сесії, то він зможе провести атаку і в зашифрованому середовищі.

2. Автентифікація – досить сильний спосіб для боротьби з перехопленням паролів. Розрізняють автентифікацію на основі багаторазових та одноразових паролів. В першому випадку статус авторизації надається тільки тому користувачу, пароль якого співпадає з паролем збереженим на сервері. При цьому бажано використовувати незвичайні та великі за розміром паролі, довжиною не менше восьми символів із використанням спеціальних символів. Більш ефективною є автентифікація на основі унікальних, одноразових паролів, які генеруються апаратним або програмним продуктом. Якщо зловмисник перехопить такий пароль, наприклад, з допомогою сніффера пакетів, то він буде абсолютно даремним, оскільки пароль вже використався і був виведений з експлуатації. Варто звернути увагу на те, що цей метод є ефективним при

боротьбі зі сніффінгом пакетів та при перехоплені паролів, але є неефективним при перехоплені іншої інформації.

3. Анти-сніффери – ефективний спосіб боротьби зі сніффінгом пакетів, який полягає в установці апаратних або програмних продуктів, які здатні виявляти сніффери, що працюють у мережі. Ці продукти не здатні зі 100% гарантією захистити мережу від загрози, але працюючи з іншими засобами мережевої безпеки, включаються в загальну систему захисту [1].

4. Антивірусні програми та мережеві екрани (фаєрволи) є особливо ефективними при боротьбі з вірусами та троянами при їх спільній роботі. Антивірус працюючий на користувацькому рівні та рівні мережі дозволяє виявляти більшість вірусів та шкідливих програм після їхньої активізації в системі та дієво знищувати їх, а фаєрвол захищає мережеві канали по яких передаються дані від несанкціонованого доступу та проникнення цих програм.

5. Використання прикладних програм. Для боротьби з парольними атаками адміністратори можуть використовувати прикладні програми, наприклад, L0phtCrack для середовища Windows, які дозволяють здійснювати аудит паролів, перевірку на надійність та їх відновлення [4].

Отже, в даному дослідженні була наведена класифікація основних мережевих атак та представлені найефективніші методи боротьби з ними, що сприяє підвищенню рівня безпеки обчислювальної техніки, яка взаємодіє з Інтернет середовищем та дозволяє запобігти проникненню шкідливих програм та несанкціонованому доступу.

Список використаних джерел:

1. Типы сетевых атак, их описания и средства борьбы [Електронний ресурс]. − Режим доступу: http://lagman-join.narod.ru/spy/CNEWS/cisco_attacks.html

2. Peng Liu. Denial of Service Attacks. – University Park. – 2004.

3. Фергюсон Н., Шнайер Б. Практическая криптография. – Москва: Вильямс, 2005. – С. 416.

4. L0phtCrack – Wikipedia, the free encyclopedia [Електронний ресурс]. − Режим доступу: https://en.wikipedia.org/wiki/L0phtCrack