ЛАБОРАТОРНА РОБОТА № 3

Тема: Безпека мережі.

Мета роботи: аналіз методів боротьби з різними видами мережевих атак та практична реалізація елементів політики мережевої безпеки (налаштування firewall, встановлення та налаштування VPN сервера).

Час виконання: 2 год.

ХІД РОБОТИ

Теоретичні відомості

Що таке мережева безпека?

Безпека мережі - це системна політика комп'ютерних мереж, яка забезпечує безпеку активів своєї організації, програмних та апаратних ресурсів. Термін мережева безпека також наголошує на моніторингу та контролі несанкціонованого доступу, неправильного використання та будь-яких небажаних змін у мережевій системі.
Найпоширеніший процес аутентифікації, що практикується повсюдно, - це присвоєння користувачеві ексклюзивного ідентифікатора і пароля для аутентифікації та доступу до ресурсів мережі.
Термін «безпека» включає як приватні мережі, так і мережі загального користування.

Що таке управління мережевою безпекою?

Управління безпекою в будь-якій мережі, будь то загальнодоступна чи приватна, - це набір політик та рутинних процедур, реалізованих мережевою системою, щоб захистити свою мережу від несанкціонованого доступу, відмови в роботі комп'ютера, перебоїв у роботі тощо, відомий як управління мережевою безпекою.
При цьому відбувається цілодобовий моніторинг мережі для запобігання системі від атак вірусів та будь-якого неправильного використання або модифікації в базі даних.
Найкращі способи управління безпекою - це використання передового антивірусного програмного забезпечення та постійне оновлення системи через регулярні проміжки часу.

Потреба в безпеці мережі

Використання Інтернету різко зросло, оскільки ми рухаємось до повної цифровізації навіть щоденних заходів. Через збільшення використання Інтернету хакери та зловмисники також активізуються, тому мережева система зазнає більшої кількості вірусних атак.
В основному, необхідність мережевої безпеки полягає у виконанні головним чином двох завдань, перше - це захист інформації від будь-якого несанкціонованого доступу, а друге - забезпечення захисту даних, що зберігаються на ПК або ноутбуках, не тільки для окремої мережі, але і для спільних або загальнодоступних мереж.
Потреба в інформаційній безпеці базується на таких моментах:

- захист інформації від небажаного доступу;
- захист даних від будь-якої невідповідної затримки маршруту, щоб доставити їх до пункту призначення у бажаний проміжок часу;
- захист даних від будь-яких небажаних поправок;
- заборона певному користувачеві мережі можливості надсилати будь-які листи, одержувач яких отримує інформацію, що вони були надіслані якоюсь третьою стороною. (Захист від приховування особи вихідного відправника).
- захист обладнання (жорсткий диск, ПК, ноутбук тощо) від атак шкідливих програм, вірусів тощо, які можуть пошкодити систему, змінивши або видаливши весь вміст, що зберігається на ньому;
- захист ПК від програмного забезпечення, яке в разі встановлення може зашкодити операційній системі, як це роблять хакери;
- захист системи від троянських коней, хробаків тощо, які можуть повністю її знищити.

Типи мережевої безпеки

Мережеву систему можна захистити різними способами, залежно від типу мережевої атаки. Для цього існує багато рішень, ряд із яких перелічено нижче:

- Антивірусне програмне забезпечення.

Захисне програмне забезпечення, яке використовується для захисту системи від вірусів, троянських атак, хробаків тощо. Це програмне забезпечення сканує систему та мережу на наявність зловмисного програмного забезпечення та атак троянських програм щоразу, коли в систему вводиться новий файл. Воно також виявляє та усуває проблему заражених даних або присутності вірусу.

- Запобігання втраті даних (DLP).

Великі організації зберігають конфіденційність даних та ресурсів, запобігаючи їхньому витоку внутрішньої інформації у зовнішній світ через власних працівників. Це робиться шляхом розгортання технології DLP, при якій адміністратор мережі обмежує доступ працівника до інформації, блокуючи порти та сайти для пересилання, завантаження або навіть друку інформації.

- Безпека електронної пошти.

Зловмисники можуть поширити вірус або шкідливе програмне забезпечення в мережі, надсилаючи його по електронній пошті. Тому потрібна висококваліфікована програма захисту електронної пошти, яка може сканувати вхідні повідомлення на наявність вірусів і здатна фільтрувати підозрілі дані та контролювати відтік повідомлень, щоб запобігти втраті будь-якої інформації системою.

- Брандмауери.

Вони є невід'ємною частиною мережевої системи. Брандмауер (між мережевий екран, фаєрвол) діє як стінка між двома мережами або між двома пристроями. В основному це набір заздалегідь визначених правил, які використовуються для запобігання несанкціонованому доступу до мережі.
Брандмауери бувають двох видів, тобто апаратні та програмні. Програмний брандмауер встановлюється в системах для захисту від різних типів атак, оскільки вони фільтрують, блокують та виправляють небажане втручання у мережу. Апаратний брандмауер діє як шлюз між двома мережевими системами, так що лише певний заздалегідь визначений користувач або трафік може отримати доступ до мережі та її ресурсів.
Система запобігання проникненню (IPS).
Це система мережевої безпеки, яка містить певний набір правил, дотримуючись яких, ви можете легко з'ясувати загрози та заблокувати їх.

- Мобільна безпека.

Кіберзлочинці можуть легко зламати або атакувати мобільні телефони за допомогою засобів передачі даних на смартфонах, вони можуть увійти в пристрій за допомогою будь-якого незахищеного посилання на ресурс веб-сайту. Тому необхідно встановити антивірус на мобільні пристрої, і люди повинні завантажувати або завантажувати дані із надійних ресурсів, а також лише із захищених веб-сайтів.

- Сегментація мережі.

З точки зору безпеки, організація, що базується на програмному забезпеченні, сегментуватиме свої важливі дані на дві-три частини та зберігатиме їх у різних місцях та на кількох ресурсах чи пристроях. Це робиться для того, щоб у гіршому випадку, якщо дані в будь-якому місці будуть пошкоджені або видалені вірусною атакою, вони могли бути знову відновлені з будь-яких резервних джерел.

- Веб-безпека.

Веб-безпека займається контролем веб-загроз, що полягає у наданні обмеженого доступу до веб-сайтів та URL-адрес шляхом блокування веб-сайтів, які є більш вразливими до вірусів та хакерів.

- Безпека кінцевої точки.

Для мережевої системи, в якій користувач, присутній на віддаленому кінці, отримує доступ до важливої бази даних організації з віддаленого пристрою, такого як мобільні телефони або ноутбуки, необхідна безпека кінцевої точки. Для цієї мети використовується різне програмне забезпечення, яке має

вбудовані вдосконалені функції захисту кінцевих точок. Це забезпечує сім рівнів безпеки.

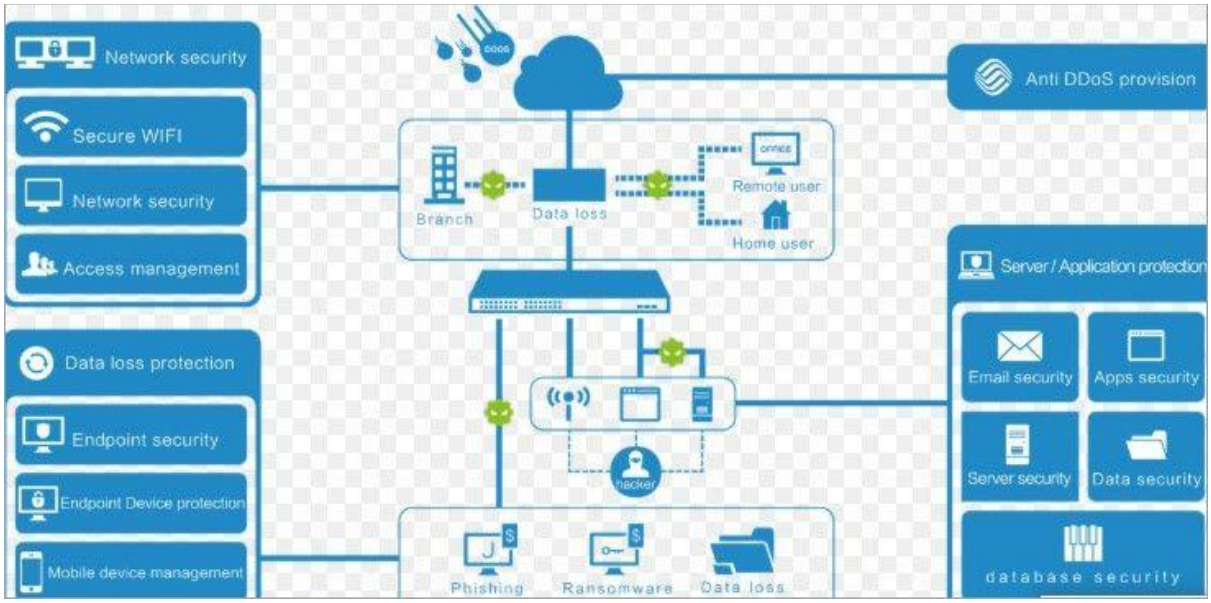
- Контроль доступу.

Мережа повинна бути спроектована таким чином, щоб не кожен мав доступ до всіх ресурсів. Це робиться шляхом розгортання захисту, такого як пароль, унікальний ідентифікатор користувача та процес аутентифікації для доступу до мережі. Цей процес відомий як контроль доступу, оскільки, реалізуючи його, ми можемо контролювати доступ до мережі.

- Віртуальна приватна мережа (VPN).

Систему можна зробити надзвичайно безпечною, використовуючи мережі VPN разом із використанням методів шифрування для автентифікації та плаваючого трафіку даних через Інтернет на віддалено підключений пристрій або мережу. IPSec - це найбільш часто використовуваний процес аутентифікації.

Типи положень безпеки на різних рівнях у системі



Як зробити систему та мережу безпечними?

Управління мережевою безпекою має бути реалізовано таким чином, що мережа буде здатною розібратися з усіма можливостями мережевих атак та проблемами, пов’язаними з вірусами, та виправити їх, відоме як.
Основними параметрами для забезпечення безпеки в системі є:
1) налаштування надійних паролів;
Щоб захистити систему або мережу від зловмисних атак, по-перше, має бути надійний пароль для входу та доступу,тобто він повинен складатися з багатьох символів, символів та цифр. Варто уникати використання дат днів народження як пароля, оскільки хакери можуть легко його зламати.
2) встановлення брандмауера;

Завжди повинен бути встановлено надійний брандмауер у мережеву систему, щоб захистити її від небажаного доступу та інших загроз.
3) антивірусний захист;
Завжди повинен бути встановлений антивірусне програмне забезпечення на систему та ноутбуки. Воно сканує, виявляє та фільтрує заражені файли, а також усуває проблему, яка виникає через вірусні атаки в системі.
4) оновлення;
Дуже важливо оновити систему та мережу останньою версією антивірусного програмного забезпечення та встановити найновіші виправлення. Це мінімізує ймовірність атаки вірусів та зробить мережу більш безпечною.
5) захисні ноутбуки та мобільні телефони.
Ноутбуки є рухомими пристроями, тому вони дуже вразливі до мережевих загроз. Так само мобільні телефони - це бездротові пристрої, і вони також легко піддаються загрозам. Для захисту цих пристроїв слід використовувати надійний пароль для доступу до різних його ресурсів. Для доступу до смарт-пристроїв буде краще використовувати біометричний пароль відбитків пальців.
6) своєчасне резервне копіювання;
Ми повинні періодично робити резервні копії файлів, документів та інших важливих даних у нашій системі або на жорсткому диску, а також зберігати їх на централізованому сервері або в якомусь безпечному місці. Це слід робити в обов'язковому порядку. У екстрених випадках це допоможе швидко відновити систему.
7) розумний серфінг на веб-сайтах;
Перш ніж завантажувати та натискати будь-яке посилання чи веб-сайт в Інтернеті, слід пам’ятати, що один неправильний клік може запустити багато вірусів у нашу мережу. Таким чином, потрібно завантажувати дані лише з надійних та захищених посилань і уникати перегляду веб-сторінок на невідомих посиланнях. Також варто уникати натискань на рекламу та пропозиції, які часто відображаються на веб-сторінці щоразу при вході в Інтернет.
8) безпечна конфігурація;
Конфігурація, виконана на IOS або маршрутизаторі, повинна виконуватися з використанням унікального ідентифікатора користувача та пароля і мусить бути захищена.
9) керування знімними носіями.
Знімні пристрої, такі як накопичувачі, ключі та картки даних, завжди повинні проходити сканування перед потраплянням у систему. Використання знімних пристроїв має бути обмеженим. Має бути розроблена така політика, за допомогою якої будь-який носій не може експортувати жодні дані із системи.

Висновок

Отже, ми дослідили необхідність мережевої безпеки, типи безпеки та ключові моменти для управління нею. Розглянуто також корисні поради як зробити мережеву систему захищеною від всіх видів вірусних та троянських атак,

застосувавши до системи надійні паролі, призначивши багаторівневу безпеку, використовуючи антивірусне програмне забезпечення та вчасно оновлюючи все програмне забезпечення та систему.

Завдання для виконання:

1. Налаштувати firewall (iptables) на віртуальному сервері з урахуванням завдань попередньої лабораторної роботи за такими параметрами:
    a. Обмежити можливість підключення по протоколу SSH тільки з вашої IP адреси.
    b. Дозволити доступ до веб сервера (http і https).

В RHEL версіях Linux (Centos, Oracle linux) за замовчуванням встановлений Firewall. За посиланням нижче інструкція як бути в цьому випадку
https://linuxize.com/post/how-to-install-iptables-on-centos-7/

2. Встановити та налаштувати VPN сервер (OpenVPN)

За посиланням нижче є скрипт автоматичного встановлення OpenVPN сервера, можна скористатися ним
https://github.com/angristan/openvpn-install

3. Продемонструвати роботу VPN сервера за допомогою утиліт traceroute чи mtr.
4. Налаштувати VPN таким чином, щоб тільки трафік в мережу 172.17.0.0/24 попадав у VPN тунель.
5. Оформити звіт про виконання роботи зі знімками екрана (або його частини), які ілюструють виконання завдань.