Лабораторна робота №4

Захист даних в комп'ютерних мережах

Мета лабораторної роботи – ознайомитися з основними поняттями комп'ютерних мереж,навчитися використовувати програмні засоби для захисту даних в комп'ютерних мережах.

1. Теоретичні відомості

Міжмережевий екран (брандмауер від нім. *brandmauer* – міцна стіна; *файрвол* від англ.*firewall* – вогненна стіна) – програмне забезпечення, розташоване на комп'ютері з метою захисту його інформаційних ресурсів або ресурсів корпоративної мережі від доступу із зовнішніх мереж. За допомогою брандмауерів можна значно підвищити мережеву безпеку і зменшити ризик для комп'ютера шляхом фільтрації небезпечних за своєю природою служб. При використанні *файрволу* комп'ютер (або локальна мережа) буде піддаватись меншому числу небезпек, оскільки *міжмережевий* екран пропускатиме тільки безпечні протоколи.

Принцип захисту комп'ютера в локальній мережі з використанням брандмауера показаний схематично на рис. 1.

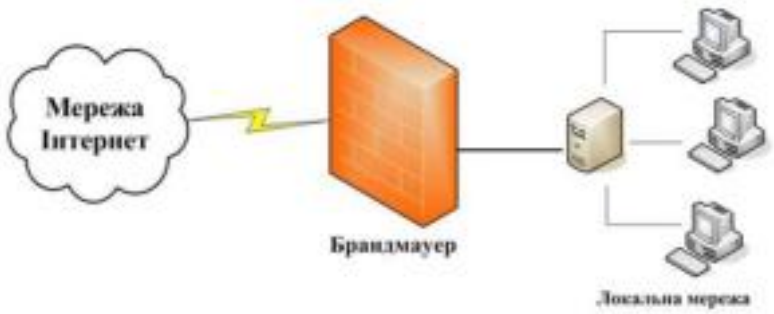

Рис. 1. Використання брандмауера

Міжмережеві екрани (*файрволи* чи *брандмауери*) є додатковою лінією захисту мереж, за допомогою яких забезпечуються всі з'єднання комп'ютера із зовнішнім середовищем, захист локальних мереж і окремих комп'ютерів від несанкціонованого доступу збоку зовнішніх мереж шляхом фільтрації двостороннього потоку повідомлень. Вони поділяються на дві великі групи:

персональні *файрволи* (брандмауери) – екрани, встановлені безпосередньо на персональні комп'ютери, які потрібно захистити

та *файрволи* (брандмауери) для захисту локальних (і корпоративних) мереж, що також називаються міжмережевими екранами.

Здебільшого, міжмережевий екран (або брандмауер) – це стратегія захисту ресурсів організації, доступних з Інтернету. При цьому він відіграє роль варти між небезпечним Інтернетом і більш надійними внутрішніми мережами. Але часто брандмауери використовуються лише для захисту сегментів Інтранет організації. У будь-якому разі їх основна функція – централізація управління доступом.

Примітка

Фактично міжмережеві екрани – це "урізані" VPN-агенти для здійснення лише фільтрації без тунелювання, оскільки в них не використовуються криптографічні методи для захисту даних. Однак, крім фільтрації, міжмережеві екрани виконують ряд додаткових функцій, зокрема:антивірусне сканування, контроль коректності пакетів, контроль коректності з'єднань(наприклад, встановлення, використання і розриву TCP-сесій), контент-контроль.

Вони можуть працювати з FTP (порт 21), e-mail (порт 25), HTTP (порт 80), NNTP (Network News Transmission Protocol, RFC 977) – протокол читання мережевих новин із багатоетапним передаванням даних (порт 119), Telnet (порт 23), Gopher – назва походить від англ. go for – система пошуку даних в мережі Інтернет (порт 70), SSL (Secure Socket Layer [Level] – рівень захищених гнізд) –протокол безпечних з'єднань (порт 443) і деякими іншими відомими протоколами. Як правило, вних не підтримується протокол прикладного рівня SNMP (Simple Network Management Protocol, простий протокол мережевого управління).

За допомогою брандмауерів забезпечують кілька типів захисту:

- блокування небажаного трафіку;

- направляння вхідного трафіку лише до надійних внутрішніх систем;
- приховування вразливих систем, які не можна убезпечити від атакз Інтернетуіншим способом;
- протоколювання трафіку у внутрішню мережу та з неї;
- приховування даних, такі як імена систем, топологія мережі, типи мережевих пристроїв і внутрішні ідентифікатори користувачів, від Інтернету;
- забезпечення більш надійної аутентифікації, ніж та, що надається через стандартні програмні додатки.

Залежно від технічного виконання і виконуваних функцій брандмауери поділяються на брандмауери з фільтрацією пакетів, брандмауери на основі машин, під'єднаних до двох мереж, брандмауери з ізольованим хостом і брандмауери з ізольованою підмережею. Брандмауер з фільтрацією пакетів є найпоширенішим і найпростішим при реалізації для маленьких мереж із простою структурою. Проте він має ряд недоліків і менш бажаний, ніж інші приклади брандмауерів. Як правило, брандмауер з фільтрацією пакетів встановлюється на маршрутизаторі з фільтрацією пакетів, через який відбувається з'єднання з Інтернет(або підмережею), на якому конфігуруються правила фільтрації пакетів, що дозволяє блокувати або фільтрувати пакети на підставі протоколів і адрес. Звичайно, з машин внутрішньої мережі надається повний доступ до Інтернету, а доступ з боку Інтернету до всіх або майже до всіх систем внутрішньої мережі блокується. Проте за допомогою маршрутизатора можна допускати вибірковий доступ до систем і сервісів (це залежить від політики). Зазвичай,блокуються такі потенційно небезпечні сервіси, як NIS, NFS і X Windows. Брандмауер з фільтрацією пакетів має ті самі недоліки, що і маршрутизатор з фільтрацією пакетів.

Примітка

NIS (Network Information Service, мережева інформаційна служба) та NFS(NetworkFile System, розподілена мережева файлова система або інколи в літературі: "системамережевих файлів", розроблена компанією Sun Microsystems Inc.; існує також: однойменнийпротокол підтримки мережевих файлових систем) – це сервіси, за допомогоюякихможназначно зменшити час, що відводиться на конфігурування хостів, управляти рядомбазданих,таких як файли паролів, за допомогою віддаленого доступу до них забезпечувати можливість спільного використання файлів і даних.

Вони спеціально розроблені для зменшення витрат на адміністрування в локальній мережі.

Брандмауер на основі машини, під'єднаної до двох мереж – краща альтернатива, ніж брандмауер на базі маршрутизатора з фільтрацією пакетів. Він складається з хосту, що має два мережеві інтерфейси, у якого відключено функцію маршрутизації IP-пакетів з одного інтерфейсу на інший (тобто з хоста не можна маршрутизувати пакети між двома мережами). Крім того, можна помістити маршрутизатор з фільтрацією пакетів між мережею і цим хостом для забезпечення додаткового захисту. Це допоможе створити внутрішню ізольовану підмережу, яка зможе бути використана для розміщення спеціалізованих систем, таких як інформаційні сервери і модемні пули . На відміну від маршрутизатора з фільтрацією пакетів за допомогою брандмауера даного типу можна цілком блокувати передавання трафіка між Інтернетом і мережею, що захищається.

Брандмауер з ізольованим хостом – більш гнучкий брандмауер, ніжтой, що побудований на основі шлюзу з двома інтерфейсами, хоча гнучкість досягається ціною де-якого зменшення безпеки. Брандмауер такого типу доречний для мереж, яким потрібна більша гнучкість, ніж та, яку може дати використання брандмауера на основі шлюзуз двома інтерфейсами. Брандмауер даного типу складається з маршрутизатора із фільтрацією пакетів і прикладного шлюзу, розміщеного в захищеній підмережі.

Брандмауер із ізольованою підмережею – це об'єднання шлюзу з двома інтерфейсами і брандмауера з ізольованим хостом. Якщо прослідкувати історію розвитку технологій міжмережевих екранів, то можна виділити кілька їх поколінь:

фільтри пакетів,
міжмережеві екрани рівня з'єднання,
міжмережеві екрани прикладного рівня,
міжмережеві екрани з динамічною фільтрацією пакетів,
міжмережеві екрани інспекції станів,
міжмережеві екрани рівня ядра,
персональні міжмережеві екрани,
розподілені міжмережеві екрани.

Спочатку технологія фільтрації пакетів застосовувалась на мережевому рівні і фільтрації

піддавались лише IP-адреси. Зараз аналіз мережевого трафіка при фільтрації пакетів проводиться і на транспортному рівні. Кожен IP-пакет досліджується на відповідність певній множині правил. За цими правилами встановлюють дозвіл зв'язку за змістом заголовків мережевого і транспортного рівнів моделі TCP/IP, аналізується і напрямок передавання пакету. За допомогою міжмережевого екрану для фільтрації пакетів часто переадресовують мережеві пакети так, що вихідний трафік проходить до інших адрес, тобто використовується схема трансляції мережевих адрес для колективного доступу до мережі (NAT – Network Address Translation). Застосування схеми NAT дозволяє сховати топологію і схему адресації довіреної мережі, а також використовувати всередині організації пул IP-адрес меншого розміру. За допомогою міжмережевих екранів рівня з'єднання перевіряють факт, що пакет є або запитом на TCP-з'єднання, або подаються дані, що мають відношення до вже встановленого з'єднання, або відноситься до віртуального з'єднання між двома транспортними рівнями. За допомогою міжмережевих екранів прикладного рівня оцінюють мережеві пакети на відповідність певному прикладному рівню перед встановленням з'єднання. За їх допомогою досліджують дані всіх мережевих пакетів наприкладному рівні та встановлюють стан повного (завершеного) з'єднання і послідовних даних. Крім того, за допомогою міжмережевих екранів можна перевіряти інші параметри безпеки, що містяться всередині даних прикладного рівня (паролі, запити служб). Брандмауери прикладного рівня повинні конфігуруватися так, щоб весь вихідний трафік здавався таким, що виходить від брандмауера (тобто щоб лише брандмауер було видно із зовнішніх мереж). У такий спосіб буде заборонений прямий доступ до внутрішніх мереж. Усі вхідні запити від різних мережевих сервісів, таких як Telnet, FTP, HTTP, RLOGIN, і т.інше, незалежно від того, який внутрішній хост запитується, повинні проходити через відповідний проксі-сервер на брандмауері. Прикладні шлюзи потребують проксі-серверів підтримуваного через брандмауер.

Використання міжмережевих екранів з динамічною фільтрацією пакетів дозволяє здійснювати модифікацію бази правил "на льоту" (on fly). Це реалізується для протоколу UDP. У цьому випадку через міжмережевий екран проводиться узгодження всіх UDP-пакетів, що проходять через віртуальне з'єднання, перетинаючи периметр безпеки. Якщо генерується пакет відповіді і передається до джерела запиту, то встановлюється віртуальне з'єднання, і пакет може надіслатися до серверу міжмережевого екрану. Дані, асоційовані з віртуальним станом, запам'ятовуються на короткий проміжок часу, тому якщо пакет відповіді не отримано, то з'єднання вважається закритим. Технологія динамічної фільтрації пакетів використовується не лише для протоколу UDP і прикладних протоколів, що спираються на нього, тому її можна назвати технологією встановлення віртуального з'єднання або віртуального сеансу.

Технологією інспекції станів (*stateful inspection*) проводиться аналіз пакетів на трьох вищих рівнях. Цей підхід використовується багатьма розробниками, але, оскільки найменування запатентоване компанією *Check Point*, вони змушені надавати йому різні найменування (крім *stateful inspection* використовуються *expert inspection, smart filtering,adaptive screening, multilevel inspection* та ін.). За допомогою пристрою інспекції станів здійснюється аналіз пакетів і формування даних про "стан віртуального з'єднання". З'єднання може знаходитись у стані встановлення, передавання або від'єднання. У кожному з цих станів є можливість інтерпретувати комунікаційні дані певним способом. Всі дані, пов'язані зі станом даного віртуального з'єднання, зберігаються в таблиці динамічних станів, за допомогою якої оцінюється подальший обмін у рамках цього віртуального з'єднання, тобто здійснюється контроль послідовності пакетів на різних рівнях. В підсистемі безпеки міжмережевих екранів, що функціонують на рівні ядра (*Kernel Proxy*), використовується багато елементів з розглянутих технологій міжмережевих екранів. Вона включає:

ядро безпеки,
модуль управління хостом,
модуль управління каналами зв'язку міжмережевого екрану,
агент реєстрації входів,
агент аутентифікації.

Основним модулем є *ядро безпеки*, за допомогою якого аналізується кожний вхідний і вихідний пакет, і яке функціонує усередині ядра операційної системи. Це дозволяє забезпечити високу продуктивність міжмережевих екранів. Розглянуті види міжмережевих екранів, особливо міжмережеві екрани прикладного рівня і рівня ядра, є надзвичайно складними та дорогими продуктами, тому для захисту комп'ютерів окремих користувачів стали розроблятися персональні міжмережеві екрани. Персональні міжмережеві екрани (їх називають також вбудованими, *embedded*) є програмними продуктами, що розташовуються в середині комп'ютера на нижчому рівні операційної системи – між мережевими платами і всіма протокольними стеками (*TCP/IP, NetBEUI, IPX* і т.ін. для *Windows*).

Персональні міжмережеві екрани, зазвичай, виконують дві основні захисні функції:
захист від зовнішніх атак і
захист від атак з боку даного комп'ютера.

Оскільки за останні роки міжмережеві екрани стали одним з основних засобів мережевого захисту, цілком природно, що хакери стали розробляти методи атак "через міжмережеві екрани" або методи атак самого міжмережевого екрану як першого рубежу оборони корпоративної мережі. Тому зусилля дослідників були спрямовані на розробку методів захисту самих міжмережевих екранів від атак ззовні. При побудові розподілених систем міжмережевих екранів їх функціональні компоненти розподіляються на вузлах мережі і можуть мати різну функціональність. При виявленні підозрілих на атаку ознак через управляючі модулі розподіленого міжмережевого екрану можна адаптивно змінювати конфігурацію, склад і розташування компонентів. В даний час розподілені системи між мережевих екранів в основному представлені лише дослідницькими прототипами. За допомогою персональних файрволів (брандмауерів) забезпечують фільтрацію вхідного та вихідного трафіка, перевірку цілісності програмних додатків, шифрування даних, захист електронної пошти від вірусів, захист комп'ютера від шпигунських програм, а також багато інших функцій, за допомогою можна убезпечити комп'ютерні інформаційні ресурси.

Після встановлення на комп'ютері файрволу, як правило, відразу помічається велика кількість спроб різноманітних дивних програм, "вирватись" в Інтернет, використовуючи для цього незвичайні порти. Це може бути шкідливе програмне забезпечення, встановлене в системі різними способами, через яке у найгіршому випадку персональний комп'ютер використовується під контролем третьої особи, що знаходиться десь в Інтернеті. Антивірусні програми часто не виявляють такого типу шкідливих програм. Встановлення файрволу на комп'ютері, під'єднаному до Інтернету, дозволить упередити всі спроби за допомогою різного шпигунського програмного забезпечення одержати доступ до даних, що зберігаютьсяв комп'ютері. Найпопулярнішими на сьогодні брандмауерами є *Outpost Firewall, ZoneAlarmPro, Kaspersky Internet Security, Kerio WinRoute Firewall, Norton Personal Firewall* та ін.

2. Загальні завдання

1. На віртуальному комп'ютері завантажити та з'ясувати призначення програмного додатку Центр безпеки (Панель керування) та компонентів, які входять до складу цього додатку.

2. Ознайомитися, налаштувати та продемонструвати роботу вбудованого брандмауера.

3. Продемонструвати увімкнення або вимкнення брандмауера Windows. Пояснити чим може загрожувати вимкнення брандмауера.

4. Перевірити проходження пакетів ICMP між комп'ютерами до і після відключення брандмауера (за допомогою команди *ping*).

5. Продемонструвати налаштування брандмауера Windows для різних типів мереж (приватна мережа, мережа спільного використання або мережа з доменами).

6. Продемонструвати надання програмі (будь-якій) дозволу на отримання даних через брандмауер.

7. Продемонструвати відкриття порту у брандмауері Windows.

8. Контрольні запитання:

Наведіть приклади класів електронної комерції і основні засоби їх безпеки.

Наведіть приклади основних сервісів, що забезпечуються зв'язком з мережею Інтернет, і засоби їх безпеки.

Надайте ваше розуміння брандмауера.

Які основні різновиди заміни мережевої адреси використовуються в брандмауерах?

9. Оформити звіт до лабораторної роботи.