Теоретичні відомості

Брандмауер (міжмережевий екран) - це система або група систем, що реалізують правила керування доступом між двома мережами. Фактичні засоби, за допомогою яких це досягається, дуже різні, але в принципі брандмауер можна розглядати як пару механізмів: один для блокування передачі інформації, а інший - для пропуску інформації. Деякі брандмауери приділяють більше уваги блокуванню передачі інформації, інші - її пропуску.

Брандмауери також важливі, оскільки дозволяють створити єдину "вразливу точку" ("choke point"), де можна організувати захист і аудит. Брандмауери забезпечують важливі функції журналізації й аудита; часто вони дозволяють адміністраторам одержувати звіти про типи й обсяги переданої через них інформації, про кількість спроб злому і т.п.

Брандмауер не може захистити від атак, що виконуються не через нього. Брандмауери не можуть захистити від передачі по більшості прикладних протоколів команд підставними ("троянськими") чи погано написаними клієнтськими програмами. Брандмауер - не панацея, і його наявність не скасовує необхідності контролювати програмне забезпечення в локальних мережах чи забезпечувати захист хостів і серверів.

Утиліта IPFW

IPFW - є системою обліку та фільтрації пакетів, що постійно знаходиться в ядрі, і має утиліту керування ipfw.

Зміна правил IPFW

ipfw [-N] інструкція [індекс] [директива] [log] протокол [опції]

Значення параметрів:

-N – Утіліта ipfw працює з адресами вузлів і номерами портів. Опція –N змушує утіліту перетворювати цю інформацію в імена, використовуючи DNS і файл /etc/services. (ця опція не є обовязковою).

інструкція – це дія, що виконується по відношенню до правила.

Допустимі інструкції:

- add – додає правило до списку;
- delete – видаляє правило зі списку;
- list – виводить весь список правил чи тльки задане правило;
- flush – видаляє всі правила зі списку, за виключенням правила по умолчанию;
- resetlog – скидає лічильник співпадінь для правила.

індекс. Це число від 0 до 65535, що означає положення правила в спску. Якщо пропустити цей параметр, система автоматично згенерує номер, який на 100 більший ніж номер останнього правила за виключенням правила по умолчанию (його номер 65535).

директива. Це дія, що виконується по відношенню до пакета. Можливі директиви:

- allow, accept і pass - директиви, що дозволяють приймати пакет (наведені директиви є синонімами, можна використовувати будь-яку для отримання того самого результату);
- deny і reject – директиви, що блокують пакет, перша змушує систему ігнорувати пакет, щоб відправник думав, що пакет загубився або компютер-адресат недоступний, друга змушує повернути відправникові повідомлення про те, що компютер або порт недоступний;
- count – директива, що змушує систему збільшити лічильники правила, але не виконувати інших дій, обробка пакету буде продовжена наступними правилами.

log. Цей параметр змушує утіліту ipfw виводити інформацію про співпадіння на системну консоль.

Протокол. Це протокол перевіряємих пакетів. Найбільш розповсюджені значення – tcp, udp, icmp. Ключовому слову Ip або all відплвідають пакети будь-якого протоколу.

Адреса. Специфікаця адреси має вигляд:

from адреса/маска [порт] to адреса/маска [порт] [via інтерфейс]

Пояснення до компонентів:

Пакет TCP/IP має адреси відправника та отримувача. Вони повинні задаватися за допомогою ключових слів from і to. Якщо ардеса не є важливою, то вкажіть ключове слово any.

Адреса може бути задана в традиційному вигляді (наприклад, 172.27.145.31) або у вигляді мережевої адреси з маскою формату CIDR (172.27.145.0/24) або маскою чотирьохбайтового формату (172.27.145.0:255.255.255.0). Ключовому слову any відповідає будь-яка адреса.

Аргумент *порт* – це номер порту для протоколів, які підтримують це поняття (TCP, UDP). Дозволяється не використовувати номер порту, вказувати декілька портів через кому або задавати діапазон портів через дефіс.

Якщо необхідно, щоб правило застосовувалося до трафіку конкретного мережевого інтерфейса, скористуйтеся ключовим словом *via*. Аргумент інтерфейс представляє собою IP-адресу або імя інтерфейса.

Опції. Утіліта ipfw підтримує різноманітні опції, що задають тип пакета. Деякі опції:

setup – цьому ключовому слову відповідають пакети, що відсилаються при спробі встановити зєднання;

in – вхідні пакети;

out – вихідні пакети;

established – ця опція дозволяє створювати правила, що дозволяють трафік у відповідь.

На початку виконання завдань введіть команду: #kldload ipfw. Вона дозволить випробовувати можливості утіліти ipfw не переконфігуровуючи ядра системи.

Приклади команд для ipfw

1. Написати команду, що змушуватиме систему приймати пакети від будь-якого комп‘ютера і пропускати пакети, адресовані будь-якому комп‘ютеру. Ця команда матиме вигляд:

ipfw add 65534 allow all from any to any

Ця команда додала правило з номером 65534.

Після введення команди на екрані ви отримаєте наступне:

65534 allow ip from any to any

Це означатиме, що правило додане.

2. Видалити певне правило зі списку (наприклад 65534). Зробити це можна наступною командою:

#ipfw delete 65534

Після введення команди на екрані ви не отримаєте жодних написів.

3. Написати команду, що дозволятиме вашому компютеру отримувати TCP-пакети з будь-якої адреси.

ipfw add 2207 allow tcp from any to 172.23.145.67

Після введення команди на екрані ви отримаєте наступне:

02207 allow tcp from any to 172.23.145.67

IP-адреса вашого компьютера буде іншою.

4. Написати команду, що дозволятиме вашому компютеру відправляти TCP-пакети на будь-яку адресу.

ipfw add allow tcp from 172.23.145.67 to any

Після введення команди на екрані ви отримаєте наступне:

02307 allow tcp from 172.23.145.67 to any

Оскільки індекс не було задано, то система сама згенерувала номер правила.

5. Написати команду, що дозволятиме вашому компютеру обмінюватися UDP-пакетами через 53-й UDP-порт з сусіднім компютером.

ipfw add 3308 allow udp from 172.23.145.66 53 to 172.23.145.67

ipfw add 3309 allow udp from 172.23.145.67 to 172.23.145.66 53

Після введення команди на екрані ви отримаєте наступне:

03308 allow udp from 172.23.145.66 53 to 172.23.145.67

03309 allow udp from 172.23.145.67 to 172.23.145.66 53

6. Продивитися список існуючих правил фільтрації пакетів.

Це можна зробити наступною командою:

ipfw list

Після введення команди на екрані ви отримаєте наступне:

02207 allow tcp from any to 172.23.145.67
02307 allow tcp from 172.23.145.67 to any
03308 allow udp from 172.23.145.66 53 to 172.23.145.67
03309 allow udp from 172.23.145.67 to 172.23.145.66 53
65535 deny ip from any to any

7. Видалити всі правила зі списку. Зробити це можна наступною командою: #ipfw flush