# Тема 2. Віртуальні машини

Поняття віртуалізації умовно можна розділити на дві фундаментально розрізняються категорії:

* віртуалізація платформ – Продуктом цього виду віртуалізації є віртуальні машини – деякі програмні абстракції, що запускаються на платформі реальних апаратно-програмних систем.
* віртуалізація ресурсів – Даний вид віртуалізації переслідує своєю метою комбінування або спрощення подання апаратних ресурсів для користувача і здобуття якихось користувальницьких абстракцій обладнання, просторів імен, мереж і т.п.

Віртуалізація ОС теж буває різна, проте нас цікавить таке її подання для користувача: в ОС фізичного комп'ютера (її прийнято називати хостовою ОС): як звичайна програма, встановлюється платформа віртуалізації, за допомогою якої створюються віртуальні машини, в яких, в свою чергу, встановлюються різні ОС (їх прийнято називати гостьовими ОС).

Під віртуалізацією платформ розуміють створення програмних систем на основі існуючих апаратно-програмних комплексів, що залежать або незалежних від них. Система, що надає апаратні ресурси і програмне забезпечення, називається хостової *(host),* а симулюючі їй системи - гостьовими *(guest).* Щоб гостьові системи могли стабільно функціонувати на платформі хостової системи, необхідно, щоб програмне і апаратне забезпечення хоста було досить надійним і надавало необхідний набір інтерфейсів для доступу до його ресурсів. Є кілька видів віртуалізації платформ, в кожному з яких здійснюється свій підхід до поняття «віртуалізація». Види віртуалізації платформ залежать від того, наскільки повно здійснюється симуляція апаратного забезпечення.

**Приклади продуктів, виконаних по технології емуляції API гостьової ОС:**

■ проект з відкритим кодом Wine (Wine Is Not an Emulator, «Wine - це не емулятор»), що дозволяє запускати DOS-, Win16-і Win32-додатки під управлінням операційної системи Linux і Unix;

■ продукт Win4Lin компанії Netraverse, що дозволяє запускати операційні системи сімейства Windows під управлінням операційної системи Linux;

■ проект з відкритим кодом DOSEMU, що дозволяє запускати DOS-додатки під управлінням операційної системи Linux;

■ проект з відкритим кодом User Mode Linux (UML), що дозволяє запускати декілька копій операційної системи Linux на одному комп'ютері (в даний час вбудований і ядро ​​Linux версії 2.6);

■ технологія Virtuozzo, розроблена російською компанією SWsoft і дозволяє запускати декілька копій операційної системи Linux на одному комп'ютері.

**Віртуальні машини з повною емуляцією гостьової ОС**

При такому вигляді віртуалізації віртуальна машина повністю виртуализует всі апаратне забезпечення при збереженні гостьової операційної системи в незмінному вигляді. Такий підхід дозволяє емулювати різні апаратні архітектури.

Проекти, що підтримують технологію повної емуляції, працюють за принципом інтерпретації інструкцій з системи команд гостьової ОС. Оскільки при цьому повністю емулюється поведінка як процесора, так і всіх зовнішніх пристроїв, то існує можливість емулювати комп'ютер з архітектурою Intel х86 на комп'ютерах з абсолютно іншою архітектурою, наприклад на робочих станціях Mac або на серверах Sun з RISC-процесорами. Головний недолік повної емуляції полягає в істотній втраті продуктивності гостьової операційної системи (швидкість роботи «гостьових» додатків може впасти в 100-1000 разів). Тому до недавнього часу ВМ з повною емуляцією найчастіше використовувалися як низькорівневі відладники для дослідження і трасування операційних систем. Однак завдяки значному зростанню обчислювальних потужностей навіть «настільних» комп'ютерів ВМ з повною емуляцією стали сьогодні цілком конкурентоспроможними. Найбільш яскравий представник цього виду ВМ - продукт Virtual PC фірми Connectix (нині купленої Microsoft).

В якості прикладів проектів, виконаних за технологією повної емуляції, можна назвати наступні:

■ проект з відкритим кодом Bochs, що дозволяє запускати різні операційні системи Intel х86 під Linux, Windows, BeOS і Mac OS;

■ продукт Simics компанії Virtutech, що дозволяє запускати і налагоджувати різні операційні системи Intel х86 під управлінням Windows та інших операційних систем;

■ проект Qemu - емулятор різних архітектур на PC,

**Часткова емуляція (нативна віртуалізація).**

У цьому випадку віртуальна машина віртуалізує лише необхідну кількість апаратного забезпечення, щоб вона могла бути запущена ізольовано. Такий підхід дозволяє запускати гостьові операційні системи, розроблені тільки для тієї ж архітектури, що і у хоста. Таким чином, кілька примірників гостьових систем можуть бути запущені одночасно. Цей вид віртуалізації дозволяє істотно збільшити швидкодію гостьових систем в порівнянні з повною емуляцією і широко використовується в даний час. Також, з метою підвищення швидкодії, в платформах віртуалізації, що використовують даний підхід, застосовується спеціальна «прошарок» між гостьовою операційною системою і устаткуванням (гіпервізор), що дозволяє гостьовий системі безпосередньо звертатися до ресурсів апаратного забезпечення. Гіпервізор, званий також «Монітор віртуальних машин» (Virtual Machine Monitor) - одне з ключових понять у світі віртуалізації. Застосування гіпервізора, що є сполучною ланкою між гостьовими системами та апаратурою, істотно збільшує швидкодію платформи, наближаючи його до швидкодії фізичної платформи.

До мінусів даного виду віртуалізації можна віднести залежність віртуальних машин від архітектури апаратної платформи.

Зазвичай програми працюють в ізольованому адресному просторі і взаємодіють з обладнанням за допомогою інтерфейсу API (Application Programming Interface - інтерфейс прикладного програмування), що надається операційною системою. Якщо дві операційні системи сумісні за своїми інтерфейсів API (наприклад, Windows 98 і Windows ME), то програми, розроблені для однієї з них, працюватимуть і на іншій. Якщо дві операційні системи несумісні за своїми інтерфейсами API (наприклад, Windows 2000 і Linux), то необхідно забезпечити перехоплення звернень додатків до API гостьової ОС і зімітувати її поведінку засобами хостової ОС. При такому підході можна встановити одну операційну систему і працювати одночасно як з її додатками, так і з додатками іншої операційної системи.

**Віртуальні машини з квазіемуляціею гостьової ОС**

Технологія квазіемуляціі гостьової ОС заснована на тому, що далеко не всі інструкції гостьової ОС потребують емуляції засобами хостової операційної системи. Багато з інструкцій, необхідних для коректної роботи «гостьових» додатків, можуть бути безпосередньо адресовані хостової ОС. Виняток становлять інструкції для керування такими пристроями, як відеокарта, IDE-контролер, таймер, і деякими іншими.

Таким чином, в процесі роботи RM з квазіемуляціей відбувається вибіркова емуляція інструкцій гостьової ОС. Очевидно, що продуктивність такої ВМ повинна бути вище, ніж у ВМ з повною емуляцією. Тим не менш, як було сказано, при досягнутих рівнях продуктивності персональних комп'ютерів різниця виявляється не настільки відчутною

# Віртуалізація ресурсів

При описі віртуалізації платформ ми розглядали поняття віртуалізації у вузькому сенсі, переважно застосовуючи його до процесу створення віртуальних машин. Однак якщо розглядати віртуалізацію в широкому сенсі, можна прийти до поняття віртуалізації ресурсів, узагальнюючим в собі підходи до створення віртуальних систем. Віртуалізація ресурсів дозволяє концентрувати, абстрагувати і спрощувати управління групами ресурсів, таких як мережі, сховища даних і простору імен.

Види віртуалізації ресурсів

**Об'єднання, агрегація і концентрація компонентів.**

Під таким видом віртуалізації ресурсів розуміється організація декількох фізичних або логічних об'єктів в пули ресурсів (групи), що представляють зручні інтерфейси користувачеві. Приклади такого виду віртуалізації:

* багатопроцесорні системи, що представляються нам як одна потужна система,
* RAID-масиви та засоби керування томами, що комбінують декілька фізичних дисків в один логічний,
* віртуалізація систем зберігання, використовувана при побудові мереж зберігання даних SAN (Storage Area Network),
* віртуальні приватні мережі (VPN) і трансляція мережевих адрес (NAT), що дозволяють створювати віртуальні простори мережевих адрес та імен.

**Кластеризація комп'ютерів та розподілені обчислення (grid computing).**

Цей вид віртуалізації включає в себе технології, які застосовуються при об'єднанні безлічі окремих комп'ютерів у глобальні системи (метакомп’ютери) для спільного вирішення загальної задачі.

**Поділ ресурсів (partitioning)**.

При поділі ресурсів у процесі віртуалізації відбувається поділ одного великого ресурсу на кілька однотипних об'єктів, зручних для використання. У мережах зберігання даних це називається зонуванням ресурсів («zoning»).

**Інкапсуляція**.

Багатьом це слово відомо як приховування об'єктом всередині себе своєї реалізації. Стосовно до віртуалізації, можна сказати, що це процес створення системи, що надає користувачеві зручний інтерфейс для роботи з нею і приховує подробиці складності своєї реалізації. Наприклад, використання центральним процесором кеша для прискорення обчислень не відбивається на його зовнішніх інтерфейсах.

Віртуалізація ресурсів, на відміну від віртуалізації платформ, має більш широкий і розпливчастий сенс і являє собою масу різних підходів, спрямованих на підвищення зручності звернення користувачів з системами в цілому. Тому, далі ми будемо спиратися в основному на поняття віртуалізації платформ, оскільки технології, пов'язані саме з цим поняттям, є в даний момент найбільш динамічно розвиваються і ефективними.

Які ж переваги несе собою можливість одночасного запуску декількох

ОС на одному комп'ютері? Ось лише деякі варіанти використання ВМ на настільних комп'ютерах користувачів:

* Робота у ВМ зі старими програмами, які не підтримують хостову ОС вашого ПК.
* Створення захищених користувальницьких середовищ для роботи з мережею (всілякі віруси й шкідливе програмне забезпечення зможе лише пошкодити ГОС ВМ, не торкнувшись реальної системи).
* Безмежний простір для експериментів (встановлюйте будь-які програми, які можуть зашкодити ОС, експериментуйте з налаштуваннями реєстру і т.д.).
* Відмінний полігон для розробки та тестування ПЗ в різних ОС і їх конфігураціях.
* Широкі можливості навчання роботі з новими ОС і програмами (наприклад, якщо вам знайома тільки Windows, ви можете собі зробити кілька віртуальних машин з різними операційними nix-системами Linux, Free BSD та QNX, запускати їх, коли потрібно, і вчитися роботі з ними).

Це, звичайно ж, далеко не всі можливості застосування ВМ на комп'ютерах користувачів. Кожен сам може собі придумати, для яких цілей йому потрібна ВМ, і відчути, наскільки це зручно, надійно і просто. Перед можливістю установки декількох ХОС на один комп'ютер з їх роздільним завантаженням, ВМ мають такі безумнівні переваги:

* Можливість працювати одночасно в декількох системах, здійснювати мережеву взаємодію між ними.
* Можливість зробити «знімок» поточного стану системи і вмісту дисків одним кліком миші, а потім протягом дуже короткого проміжку часу повернутися в початковий стан.
* Простота створення резервної копії ОС (не треба створювати ніяких образів диску, всього лише потрібно скопіювати папку з файлами ВМ).
* Можливість мати на одному комп'ютері необмежене число віртуальних машин з абсолютно різними операційними системами і їх станами.
* Відсутність необхідності перезавантаження для перемикання в іншу ОС.

Тим не менш, незважаючи на всі переваги, ВМ також мають і недоліки:

* Потреба в наявності достатніх апаратних ресурсів для функціонування декількох ОС одночасно.
* ОС працює трохи повільніше у ВМ, ніж на «голому залізі». Однак, останнім часом показники продуктивності гостьових систем значно наблизилися до показників фізичних ОС (в межах одних і тих же ресурсів), і незабаром, за рахунок поліпшення технологій реалізації віртуальних машин, продуктивність гостьових систем практично буде рівна реальним.
* Існують методи визначення того, що програма запущена у ВМ (в більшості випадків, виробники систем віртуалізації самі надають таку можливість). Вірусорозробники і розповсюджувачі шкідливого ПЗ, звичайно ж, в курсі цих методів і останнім часом включають в свої програми функції виявлення факту запуску у ВМ, при цьому ніякої шкоди ворожливе ПЗ гостьовій системі не заподіює.
* Різні платформи віртуалізації поки не підтримують повну віртуалізацію всього апаратного забезпечення та інтерфейсів. Останнім часом кількість підтримуваного апаратного забезпечення стрімко зростає у всіх виробників платформ віртуалізації. Крім основних пристроїв комп'ютера, вже підтримуються мережеві адаптери, аудіоконтроллер, інтерфейс USB 2.0, Котролер портів COM і LPT і приводи CD-ROM. Але найгірше йдуть справи з віртуалізацією відеоадаптерів і підтримкою функцій апаратного прискорення тривимірної графіки - у віртуальних машинах все ще повноцінно не можна грати в 3D гри! У цьому плані, попереду всіх знаходиться компанія VMware з експериментальної підтримкою функцій Direct 3D (проте, деякі важливі функції, такі як Vertex-шейдери все ще не підтримуються). Але в найближчому майбутньому ця проблема, безумовно, буде вирішена.

Всі перераховані недоліки ВМ в принципі можуть бути розв'язані і, в порівнянні з великим переліком їх переваг, є не настільки істотними. Саме тому, технології віртуалізації і ВМ розвиваються вибуховими темпами, а користувачі знаходять їм все нові і нові застосування.

**ПЕРЕВАГИ ТА НЕДОЛІКИ ВИКОРИСТАННЯ ВІРТУАЛЬНИХ МАШИН**

**Переваги:**

**1. Економія на апаратному забезпеченні при консолідації серверів.**

Істотна економія на придбанні апаратного забезпечення відбувається при розміщенні декількох віртуальних серверів на одному фізичному. Залежно, від компанії-постачальника платформи віртуалізації, доступні можливості по балансуванню робочого навантаження, контролю виділених ресурсів, міграції між фізичними хостами і бекапа. Все це тягне за собою реальну економію коштів на обслуговуванні, управлінні та адмініструванні інфраструктури серверів.

Не потрібно міняти кулери на процесорах, ремонтувати вийшов з ладу блок живлення і т.д. і т.п. З іншого боку підвищується вимогливість до апаратних ресурсів (мінус). У разі розміщення на одному фізичному і безлічі віртуальних серверів різних ОС і додатків ми виграємо наступне:

**Обладнання для системи займає менше місця в стійці.**

Замість стійки в 3-4 малопотужних сервера можна встановити один сервер, який буде виконувати ті ж самі функції. Особливо це критично, якщо обладнання розміщується на орендованій майданчику провайдера або не вистачає місця в стійці. Для віртуальних машин, розміщених на одному сервері, потрібно менше портів на KVM-switch (Keyboard-Video-Mouse).

**Додаються додаткові можливості адміністрування.**

Наприклад, з'являється можливість при зависанні програми не тільки перезапустити потрібні процес, а перезавантажити віртуальний сервер цілком, не впливаючи на роботу додатків, розміщених на інших віртуальних серверах.

**Поліпшується система безпеки.**

Навіть при успішному несанкціоноване проникнення по мережі на один віртуальний сервер інші віртуальні сервери залишаються недоторканими.

**Значно спрощується процес делегування повноважень.**

Можна передати права на адміністрування віртуальним сервером довіреній особі, яка не переживаючи про перетин повноважень при управлінні процесами, розміщеними на інших серверах.

1. **На одному комп'ютері можливе використання серверів під управлінням різних операційних систем,** наприклад, Windows і FreeBSD.
2. **Можливість підтримки старих операційних систем з метою забезпечення сумісності.**

При виході нової версії операційної системи, стару версію можна підтримувати на віртуальній машині, поки не буде повністю обкатана нова ОС. І навпаки, можна «підняти» нову ОС на віртуальній машині і випробувати її без шкоди для основної системи.

1. **Можливість ізолювати потенційно небезпечні оточення.**

Якщо якийсь додаток або компонент викликає сумніви в його надійності і захищеності, можна використовувати його на віртуальній машині без небезпеки пошкодити життєво важливі компоненти системи. Таку ізольоване середовище називають також «пісочницею» *(sandbox).* Крім цього, можна створювати віртуальні машини, обмежені політиками безпеки (наприклад, машина перестане запускатися через два тижні).

1. **Можливість створення необхідних апаратних конфігурацій.**

Іноді потрібно використовувати задану апаратну конфігурацію

(процесорний час, кількість виділеної оперативної і дискової пам'яті) при перевірці працездатності додатків в певних умовах. Досить складно без віртуальної машини «загнати» фізичну машину в такі умови. У віртуальних машинах - це пара кліків миші.

**6 Віртуальні машини можуть створювати уявлення пристроїв, яких у вас немає.**

Наприклад, багато систем віртуалізації дозволяють створювати віртуальні SCSI диски, віртуальні багатоядерні процесори і т.п. Це може стати в нагоді для створення різного роду симуляцій.

1. **На одному хості може бути запущено одночасно кілька віртуальних машин, об'єднаних у віртуальну мережу.**

Така особливість надає безмежні можливості по створенню моделей віртуальної мережі між декількома системами на одному фізичному комп'ютері. Особливо це необхідно, коли потрібно змоделювати якусь розподілену систему, що складається з декількох машин. Також можна створити декілька ізольованих користувальницьких оточень (для роботи, розваг, роботи в Інтернет), запустити їх і перемикатися між ними в міру необхідності виконання тих або інших завдань.

1. **Віртуальні машини підвищують мобільність.**

Папка з віртуальною машиною може бути переміщена на інший комп'ютер, і там віртуальна машина може бути відразу запущена. Не потрібно створювати ніяких образів для міграції, і, до того ж, віртуальна машина відв'язана від конкретної апаратури.

**9 Віртуальні машини більш керовані.**

При використанні віртуальних машин істотно підвищується керованість щодо створення резервних копій, створення знімків станів віртуальних машин («снепшот») і відновлень після збоїв у зв'язку з тим, що сервери служб отримують незалежність від заліза, на якому працюють.

# Недоліки

На цьому, звичайно, гідності віртуальних машин не вичерпуються, це лише їжа для роздумів і дослідження їх можливостей. Безумовно, як і у всякого нового і перспективного рішення, у віртуальних машин є і свої недоліки:

1. Неможливість емуляції всіх пристроїв.

В даний момент всі основні пристрої апаратних платформ підтримуються вендорами систем віртуалізації, однак якщо ви використовуєте, наприклад, будь які контролери або пристрою, які не підтримуються ними, доведеться відмовитися від віртуалізації такого оточення.

1. Віртуалізація вимагає додаткових апаратних ресурсів.

В даний час використання різних технік віртуалізації дозволило наблизити показники швидкодії віртуальних машин до реальних, однак, щоб фізичний хост зміг запускати хоча б пару віртуальних машин, потрібна достатня для них кількість апаратних ресурсів.

1. Деякі платформи віртуалізації вимогливі до конкретного апаратного забезпечення.

Зокрема, чудова платформа компанії VMware, ESX Server, була б і зовсім чудовою, якби не висувала жорстких вимог до апаратного забезпечення.

4 Хороші платформи віртуалізації стоять хороших грошей.

Часом, вартість розгортання одного віртуального сервера дорівнює вартості ще одного фізичного, в певних умов це може виявитися недоцільним. На щастя, є безліч безкоштовних рішень, але вони, в основному, орієнтовані на домашнього користувача і малий бізнес.

**СФЕРИ ЗАСТОСУВАННЯ ВІРТУАЛЬНИХ МАШИН**

# Віртуальні сервери

Як можна використовувати віртуальну машину в корпоративній або офісної мережі? Наприклад, підняти віртуальний сервер. Припустимо, нам потрібен публічний WEB та приватний SQL. З міркувань безпеки, публічний сервер повинен бути розташований в так званій демілітаризованій (DMZ) зоні, а приватний SQL - всередині локальної мережі, обнесеній по периметру глибоким захисним ровом (брандмауером). Що вимагає двох машин. А як бути, якщо в наявності є тільки одна?

Теоретично, можна підняти VMware або Virtual PC, розмістивши публічний WEB-сервер на віртуальній машині, а приватний SQL - на основній. І це як би буде працювати. «Як би» - тому що для досягнення прийнятного рівня продуктивності навіть за підтримки апаратної віртуалізації нам знадобиться досить потужне залізо, здатне тягнути емулятор з розумною швидкістю.

# Загін для вірусів

Досить часто ВМ використовуються для експериментів з потенційно небезпечним програмним забезпеченням, отриманим з ненадійних джерел. Антивірусна перевірка - не дуже-то хороший засіб для пошуку невідомих або модифікованих черв'яків, вірусів і руткітів. Шкідникам добре відомо, як «засліпити» проактивні технології та евристичні аналізатори. Утиліти, орієнтовані на пошук руткітів, добре працюють лише в перші дні своєї появи, а потім хакери знаходять обхідний шлях.

Пряме порівняння дискових образів палить всі руткіти, черв'яки і віруси

без винятку (звичайно, за умови, що вони вносять зміни в файлову систему, а не обмежуються зараженням однієї лише оперативної пам'яті, вмираючи при перезавантаженні). Алгоритм пошуку зарази виглядає так: знімаємо образ стерильної системи, зберігаючи його в надійному місці, встановлюємо нове програмне забезпечення, знімаємо ще один образ. Монтуємо обидва образи на свідомо не заражену систему і порівнюємо їх. Тривіальне Пофайлове порівняння виявляє до 90% малварі. Інші 10% виявляє побайтово порівняння, «витягувати» віруси, які ховаються в NTFS-потоках або інших місцях (працюючи з диском на низькому рівні, ми повинні знати всі базові структури файлової системи, докладно описані в моїй книзі «Техніка відновлення даних», електронну копію якої можна безкоштовно завантажити тут: nezumi.org.ru / recover-full-rus.zip).

Природно, проводити подібні експерименти найкраще під емулятором. Так набагато простіше оперувати образами віртуальних жорстких дисків, та й виділяти окрему (фізичну) машину не буде потрібно. Зручність, простота і економія - очевидна. Але простота гірша за крадіжку, і економія на виділеній машині до добра не доводить. Якщо ВМ з'єднана з основною системою віртуальної мережею, то черв'яки можуть атакувати базову ОС, використовуючи діри в мережевих службах. Адміністратору слід або своєчасно встановлювати всі заплатки, або відключити вірусний загін від Мережі взагалі - не забуваючи про Розшарені ресурси. Віртуальна машина VMware підтримує їх в обхід Ethernet-адаптера. Кулі продовжують працювати навіть після видалення віртуальної мережевої карти, і схильні відразу двом типам атак - через діри в сервісі «загальних папок» і шляхом засилання черв'яків, модифікуючих шаблон папки, автоматично «підхоплює» Провідником. Те ж саме відноситься і до всіх інших типів носіїв. Це істотно ускладнює обмін даними між віртуальною і основний машинами. Саме надійне - копіювати дані через CD-ROM (не обов'язково фізичний - підійде і віртуальний, просто беремо будь-яку програму для створення iso-образів і монтуємо її на основну систему і на VMware).

Важливо: за замовчуванням VMware автоматично розпізнає всі підключаємі USB-пристрої і дає ВМ до них повний доступ. Припустимо, ми підключаємо FLASH, зовнішній жорсткий диск з USB-інтерфейсом або інший девайс подібного роду, на якому тут же оселяється вірус, що вирвався з катівень віртуальної машини. Щоб запобігти вторгненню, достатньо відключити USB-контролер у властивостях віртуальної машини.

Однак проблеми на цьому не закінчуються. Руткіти вже давно навчилися розпізнавати ВМ, відмовляючись від зараження в їх присутності, що ламає весь концепт. Ми встановлюємо програмне забезпечення з руткітам на віртуальну машину, порівнюємо образи, нічого не знаходимо і, задоволені собою, запускаємо руткіта в основну систему. Виходить, гарантовано виявити сучасних руткітів за допомогою віртуальних машин неможливо! А якщо ще врахувати велику кількість дірок в емуляторах, то руткіт має всі шанси заразити основну систему з гостьової машини. Вихід? Або використовувати виділену живу машину, або надійну віртуальну машину з повною емуляцією (наприклад, Bochs). Це запобіжить вірусному вторгненню, але, на жаль, не врятує від детекції ВМ руткітам. Bochs містить безліч дрібних дефектів емуляції (веде себе не як справжній процесор), які не перешкоджають роботі нормальних програм, але можуть бути використані для Детектив емулятора. До того ж, БУДЬ емулятор несе на своєму борту досить специфічний набір віртуального заліза, за яким його легко впізнати. І хоча за наявності вихідних текстів ми можемо перешкодити цьому - купити живий комп'ютер набагато дешевше, ніж жолобити віртуальне залізо.

Резюмуючи вищесказане, робимо висновок: віртуальні машини - не дужето надійний загін для вірусів, хоча якщо не бути параноїком, то (з урахуванням низької якості переважної більшості вірусів і руткітів) краще використовувати віртуальну машину, ніж цілком покладатися на антивіруси.

# Інструмент виявлення мережевих атак

Офісні мережі зазвичай не відчувають необхідності в сенсорах і датчиках, детектирующих вторгнення, а якщо і відчувають, то справа зазвичай обмежується придбанням комерційної IDS/IPS-системи, вбудованої в брандмауер і спокійно працює на шлюзі в інтернеті або на одному з вузлів локальної мережі.

З ростом мережі з'являється бажання встановити спеціалізовану систему виявлення вторгнень, наприклад, Snort (безкоштовний) або AMP (комерційний). І розмістити її на виділеному вузлі, оскільки для установки того ж AMP адміністратор повинен надати його постачальникам віддалений shell на свою машину. Причому, AMP буде не тільки автоматом завантажувати свіжі сигнатури з Мережі, але і відправляти весь підозрілий трафік для аналізу на сервери компанії Endeavor, яка і є його розробником.

Довіра - це прекрасно, але віддавати свій трафік в чужі руки ... Ні, краще розмісити цю штуку на окремому вузлі, відключеному від основної локальної мережі, але живити від того ж самого ISP - тобто що ловить тих же вірусів і черв'яків, що і основні вузли локальної мережі. Чи можна використовувати для цієї мети віртуальну машину? Звичайно! Головне, надійно ізолювати її від корпоративної мережі.

Найбільшу проблему становлять віртуальні мережеві карти, через які гостьова операційна система легко добереться до основної. Всі віртуальні картки в обов'язковому порядку повинні бути відключені! Але ... якщо у нас немає мережі, як же тоді спілкуватися із зовнішнім світом і ловити трафік? Варіантів багато. Ось тільки один з них: ADSL-модем з USB-інтерфейсом, підключений до віртуальної машини з висмикнутою мережевою картою і заблокованими кулями.

Яку саме віртуальну машину слід використовувати? VMware дуже відома і занадто діряве. Bochs неймовірно повільно працює. Virtual PC - непоганий вибір, але враховуючи велику кількість дірок в процесорах, його використання вкрай небезпечно. Реально залишається тільки VirtualBox, XEN або QEMU.

# Дзеркальний сервер

Шкідлива природа черв'яків і вірусів цілком з'ясовна. Вони якраз для цього і писалися. На жаль, чесне програмне забезпечення часто завдає набагато більшої шкоди. Взяти хоча б оновлення безпеки або нові версії. Всім адміністраторам добре відомо, що їх установка деколи приводить до важковирішуваними конфліктів, втрат даних, а то й повного краху операційної системи!

Аналогічним чином справи йдуть з крученням налаштувань, сенсу яких адміністратор до кінця не розуміє і діє методом тику. Один невірний рух руки - і система відмовляється завантажуватися, а щоб підняти її, потрібні знання та кваліфікація, що виробляються тільки в боротьбі з ось такими злетами і падіннями. По книжках всього не вивчиш ... І тут віртуальні машини - незамінні.

Просто встановлюємо систему з усіма додатками та сервісними службами на VMware / Virtual PC / VirtualBox / etc, і всі нові латочки, поновлення, настроювання, в першу чергу, обкатуємо на гостьовий операційній системі, спостерігаючи за її реакцією. Якщо політ нормальний - переносимо зміни на основну машину. Якщо ж ні - міркуємо, що тут не так, і де косяк.

Віртуальні машини відкривають практично необмежені можливості для експериментів. Головне - правильно ними скористатися, передбачивши максимум можливих побічних ефектів і розробивши план щодо їх усунення.

Існуючі віртуальні машини призначені для запуску чесних додатків і чисто конструктивно не пристосовані для ізоляції шкідливого програмного забезпечення. А тому використовувати їх у ролі «пісочниці» (своєрідного загороди для вірусів) категорично не рекомендується, а якщо і використовувати, то тільки з купою пересторог, описаних вище.

Навіть самий крутий руткіт не встоїть проти порівняння дискових образів (за вирахуванням руткітів, що мешкають виключно в оперативній пам'яті і не вносять у файлову систему ніяких змін). Проблема в тому, що руткіти вже навчилися детектувати популярні віртуальні машини, відмовляючись від вторгнення в їх присутності. А тому, чим менше відома віртуальна машина, тим краще для адміністратора і гірше для руткіта.

**ОГЛЯД ВІРТУАЛЬНИХ МАШИН**

# VirtualBox

VirtualBox - програмний продукт німецької компанії innotek. Це порівняно молода платформа, перший публічний реліз випущений в січні 2007 р. Серед підтримуваних гостьових систем - Windows, Linux, OS / 2 Warp,

OpenBSD і FreeBSD. У лютому 2008-го фірма innotek була придбана компанією Sun Micro-systems, і подальша розробка ведеться з її участю. Модель поширення VirtualBox при цьому не змінилася.

Крім стандартних і необхідних для роботи операційної системи пристроїв (процесор, відеоадаптер, жорсткий диск), програма також емулює аудіоконтроллер і мережевий адаптер. Останній представляється як інтерфейс AMD PCNet. Крім того, необхідно відзначити, що за замовчуванням відеокарта емулюється як стандартний VESA-адаптер з 8 МБ відеопам'яті і роздільною здатністю 800 × 600; якщо ж цього недостатньо, можна скористатися Guest VM Additions для збільшення продуктивності віртуального відеоакселератора і динамічної зміни розмірів вікна. Guest VM Additions - поставляється разом з програмою набір засобів для оптимізації швидкодії і полегшення взаємодії між гостьовою і хостовой ОС. Крім всього в VirtualBox емулюються також контролери USB, при цьому пристрої, підключені до USB-роз'ємів в хостовой системі, автоматично підхоплюються і в гостьовій.

Однією з ключових можливостей є підтримка RDP (Remote Desktop Protocol), що дозволяє VirtualBox діяти як RDP-сервер і управлятися будь-яким клієнтом, що працюють з даним протоколом. Зауважимо, що до виходу платформи VMware Workstation 6 ця можливість була тільки у VirtualBox. Також реалізована функція USB over RDP (якщо віртуальна машина діє як RDP-сервер, то в клієнті будуть видні і підключення USB-пристрою).

Другий ключовою особливістю є компонент iSCSI initiator. Він дозволяє використовувати зовнішні пристрої за протоколом iSCSI в якості віртуальних дисків в гостьовій системі без додаткової підтримки з її боку.

Процес створення віртуальної машини гранично простий: необхідно вибрати тип операційної системи і встановити обсяг оперативної пам'яті і жорсткого диска. Останній може бути як фіксованого розміру, так і динамічно змінюваний в міру заповнення. Після інсталяції гостьової системи рекомендується встановити вже згадувані Guest VM Additions - вони суттєво полегшать роботу надалі.

VirtualBox підтримує мережеву взаємодія між віртуальними машинами, при цьому користувач вольний вибрати один з трьох типів. Перший - це NAT, в такому випадку віртуальна машина прихована за NAT-сервером хоста і може ініціювати з'єднання в зовнішнє по відношенню до нього мережу, але з зовнішньої мережі з'єднатися з такою віртуальною машиною можна. Другий тип, Host Interface Networking, дозволяє гостьовій системі використовувати ресурси фізичного мережевого адаптера хоста, при цьому сама гостьова машина стає доступна з зовнішньої мережі як звичайний незалежний комп'ютер. І нарешті, третій тип - Internal Networking - може використовуватися, коли необхідність у виході в зовнішню мережу немає; в цьому випадку віртуальна мережа буде побудована в межах хоста. Якщо ж користувачеві потрібно всього лише налагодити обмін файлами між гостьовою системою та хостом, то краще застосувати функцію Shared Folders, яка дозволяє створювати загальні папки, доступні в будь-який з систем.

Ті, хто використовує віртуальні машини для тестування різного програмного забезпечення, по достоїнству оцінять підтримку древа збережених станів віртуальної машини (так звані snapshots), до яких може бути проведений відкат з будь-якого стану гостьової системи у разі непередбаченої ситуації або необхідності в її перезапуску з нуля.

Для розробників компанія innotek надає відмінний Software Development Kit, і оскільки код платформи відкритий, докладати додаткових зусиль для написання розширень до системи не потрібно. Крім Windows, стабільні версії VirtualBox існують також для Linux і Mac OS. Підсумовуючи все вищесказане, можна з упевненістю назвати VirtualBox кращою з безкоштовних програм в своїй області і серйозним конкурентом для платних аналогів.

# VMware Workstation

VMware Workstation - мабуть, найвідоміший продукт для створення віртуальних машин, а компанія VMware на сьогоднішній день є одним з лідерів у виробництві систем віртуалізації. Список сумісних гостьових ОС просто величезний - тут є все, починаючи від Solaris і Novell NetWare і закінчуючи Linux, FreeBSD і Windows Vista x64 Edition. Платформа прекрасно емулює всі необхідні системи комп'ютера. Кількість підтримуваних пристроїв не може не радувати - VMware Workstation здатна працювати з встановленими CD / DVDприводами, дисководами, зчитувачами смарт-карт, вміє монтувати образи дисків. Крім того, в гостьовій системі будуть доступні всі зовнішні пристрої, підключені через COM-, LPT-або USB-порти (правда, налаштувати підтримку USB 2.0 так і не вдалося). Присутня повна інтеграція з ACE (Assured Computing Environment - можливість запускати на комп'ютері ще одну копію Windows, призначену для спільного використання) і так званий unity mode - виконання віртуалізованих додатків на Робочому столі хост-машини. Що ж стосується традиційно слабкого місця - відеоакселератора, - то, починаючи з поточної версії, він підтримує апаратне прискорення тривимірної графіки. Правда, з невеликим застереженням - поки ця функція доступна лише при використанні Windows XP в якості гостьової операційної системи. Також в даний час підтримується тільки DirectX 9.0 і Shader Model 2.0. Ще серед останніх нововведень варто відзначити можливість потокового відтворення віртуальної машини, наприклад при завантаженні образу з Інтернету.

Обмін даними може бути організований через віртуальну локальну мережу або ж за допомогою drag-n-drop з віртуальної системи в напрямку хоста. У випадку з локальною мережею є три стандартні варіанти: перший з використанням NAT (Network Address Translation), другий - безпосередньо в існуючу мережу, і третій - віртуальна мережа в межах хоста. Зрозуміло, не забута і можливість створення спільних папок.

Для тестуючих ПP в VMware Workstation реалізований механізм створення миттєвих знімків (snapshots) операційної системи і дисків, які згодом можуть бути використані для відкату в одне з попередніх станів. Є тут і підтримка дерев таких знімків, що неймовірно зручно при конфігуруванні системи з різними надбудовами (наприклад, різними версіями браузера Internet Explorer). Крім того, в новій версії були істотно поліпшені засоби налагодження, які дозволяють у реальному часі записувати всю роботу машини, включаючи активність додатків, процесора і інших апаратних засобів, а також відтворювати збережені дані.

У комплекті з програмою поставляється ще одна воістину незамінна утиліта - P2V Assistant, яка дозволяє буквально в пару кліків перетворити фізичну систему в віртуальну.

Варто відзначити, що саме WMware продемонструвала найвище швидкодію, хоча швидкість завантаження залишає бажати кращого. Ще одним недоліком програми є її ціна. Правда, є безкоштовна версія - VMware Player, що дозволяє запускати раніше збережені віртуальні системи, однак не вміє їх створювати.

# Microsoft Virtual PC

Microsoft Virtual PC міг би стати гідним конкурентом програмами, представленим в огляді, якби не одне «але» - підтримка в якості гостьових систем тільки відносяться до сімейства Windows, що істотно обмежує область застосування даного емулятора. При бажанні можна встановити непідтримуванe ОС, вибравши при установці пункт Other, однак коректна робота в такому випадку не гарантується. Як і всі розглянуті в огляді програми, Virtual PC містить набір додатків, покликаних полегшити життя користувачу. В даному випадку це Virtual Machine Additions - їх установка не збільшить швидкодії гостьової системи, але зробить доступними наступні корисні та зручні функції:

* можливість перетягування за допомогою технології drag-n-drop файлів і папок з хостовой системи в гостьову і назад;
* при зміні розмірів вікна з гостьовою системою дозвіл всередині неї буде автоматично підганяти під новий розмір;
* поліпшений драйвер віртуального відеоадаптера дозволить

встановити довільні дозвіл і глибину кольору;

* фокус миші буде автоматично передаватися в гостьову систему при попаданні курсору в межі вікна консолі і повертатися в хостовую при виході з цієї зони. Це позбавить від необхідності натискати правий Alt для того, щоб передати фокус в гостьову систему, і дозволить працювати з вікном консолі гостьової системи як із звичайним додатком;
* для обміну файлами з хостовой операційною системою можна буде використовувати загальні папки (Shared Folders);
* буфер обміну у гостьовій і хостовой систем також стане загальним, що дозволить спростити взаємодію додатків хоста і гостьової системи;
* з'явиться синхронізація часу між хостовой і гостьової системами.

Враховуючи повну безкоштовність продукту, його можна сміливо рекомендувати для домашнього використання.