электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.453

Настройка испытательного стенда для проведения оценки эффективности функционирования средств защиты информации от НСД на основе средств виртуализации

Строганов И.С., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Алешин В.А., к. т. н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
v.a.matveev@bmstu.ru

Поскольку исследуются различные методы защиты информации от несанкционированного доступа (НСД) и разрабатываются различные системы обнаружения вторжений (СОВ), то очевидным преимуществом было бы иметь средства оценки успешности этих систем в обнаружении атак.

Наилучшая среда для тестирования и оценки системы обнаружения вторжений – это та среда, в которой она будет использоваться.

Однако группы исследователей обычно не имеют доступа к рабочим сетям для тестирования своих систем, и эти системы (особенно пока они находятся в начальной стадии разработки) тестируются в симулированной среде.

Схема испытательного стенда для проверки систем обнаружения вторжений представлена на рис.1.

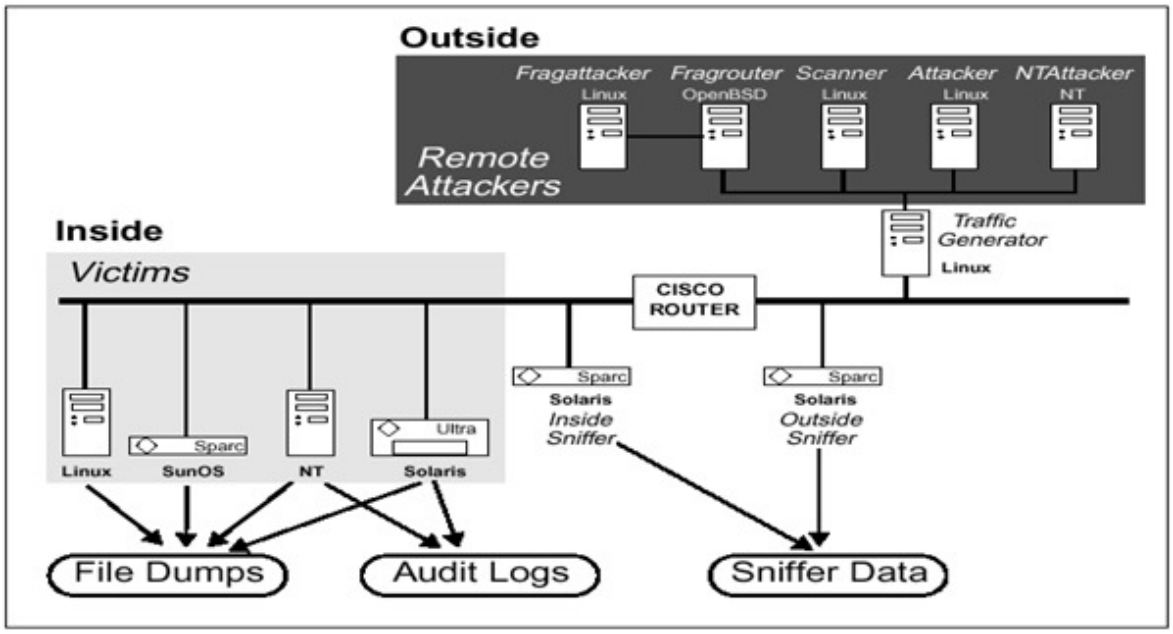

Рис. 1. Схема стенда для проверки эффективности СОВ 1998-1999, проведенной Lincoln Laboratory MIT в рамках проекта по заказу DARPA

Представленный стенд можно реализовать на основе использования современных средств виртуализации.

Существует два основных способа виртуализации на компьютерной архитектуре x86. В первом случае (рис.2,а) гостевая операционная система (ОС) находится над слоем виртуализации, работающим как приложение базовой ОС. Во втором случае (рис.2,б) гостевая ОС находится над слоем виртуализации, входящим в состав гипервизора – программного обеспечения, работающего на том же уровне, что и базовая операционная система.

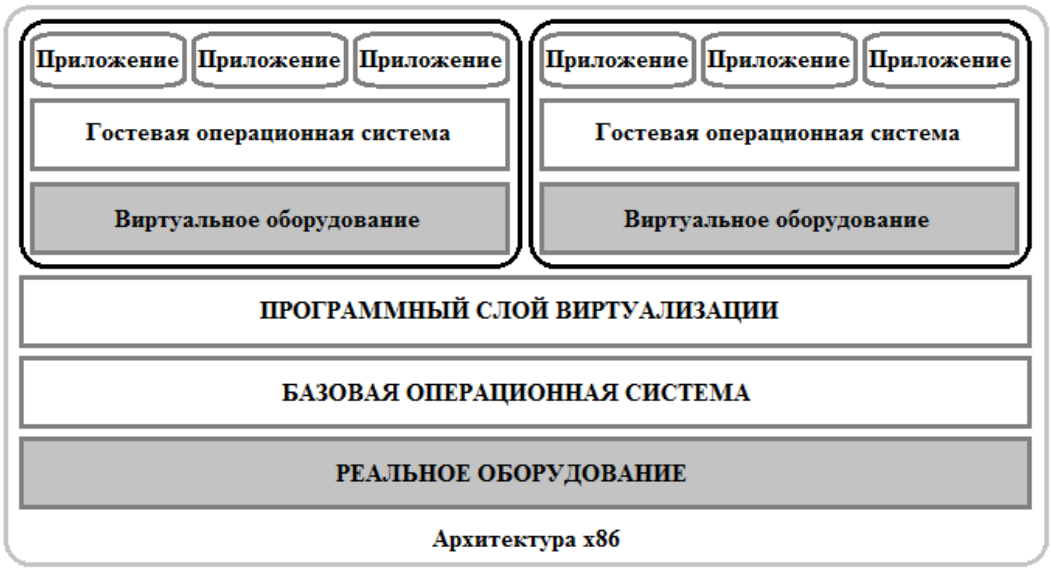

Рис. 2,а. Первый подход к виртуализации вычислительного процесса

Рис. 2,б. Второй подход к виртуализации вычислительного процесса

К реализациям первого способа относятся продукты VMware Server, VirtualBox, Microsoft Hyper-V, Parallels Workstation, а к реализациям второго – VMware ESX Server, Xen, Citrix XenServer, Oracle VM Server. В некоторых серверах встроенное программное обеспечение может содержать гипервизор.

Существует метод полной виртуализации, который использует бинарную трансляцию команд, и метод паравиртуализации. Основная идея паравиртуализации заключается во взаимодействии гостевой ОС с гипервизором для улучшения производительности и работы с памятью. Для этого гостевую операционную систему модифицируют, заменяя некоторые участки кода на гипервызовы к гипервизору. Относительно новым методом является встроенная поддержка виртуализации в современном оборудовании. Как показано на рис.2,в, данные технологии наделяют монитор виртуальной машины (МВМ) большим приоритетом выполнения, чем у программ уровня Ring 0.

Рис. 2,в. Подход к использованию встроенной виртуализации

Команды, поступающие от виртуальных машин, автоматически перехватываются МВМ и обрабатываются необходимым образом, что избавляет от необходимости полной бинарной трансляции или паравиртуализации.

В целом, чем больше число виртуальных машин, тем больше нагрузка на процессор. При использовании одной виртуальной машины нагрузка минимальна и может составлять до 15%, в этом случае вычислительные мощности компьютера используются неэффективно.

Динамики улучшения характеристик выпускаемых процессоров и оперативной памяти являются линейными, однако прирост вычислительных мощностей процессора больше, чем прирост объемов оперативной памяти за одинаковый период. К тому же зависимость стоимости составляющей ОЗУ в серверах от объема оперативной памяти напоминает геометрическую прогрессию. Таким образом, стоимость эффективного сервера для виртуализации во многом определяется стоимостью оперативной памяти.

Поэтому в качестве подхода к построению испытательного стенда можно использовать технологии виртуализации. Наиболее доступными являются продукты линейки VMware.

Основные функции стенда:

1. Проведение исследований по оценке эффективности в любой имеющейся функциональной (операционной) среде и сетевой архитектуре.

2. Проведение сертификационных испытаний средств защиты информации от НСД в рамках задач, выполняемых лабораторией «МГТУ-ТЕСТ» (кафедра ИУ8).

Цели и задачи проверки:

1. Контроль средств защиты информации от НСД и операционных систем (ОС) на наличие уязвимостей.

2. Анализ возможностей и реализация средств тестирования выявленных уязвимостей.

3. Оценка эффективности средств защиты.

Основные подходы к разработке стенда:

1. На стенде должны быть реализованы две подсети, соединённые с помощью маршрутизаторов (роутеров).

2. Одна из подсетей считается «внешней», а другая «внутренней».

3. Целевая система (тестирование которой и проводится) находится во внутренней сети, а внешняя сеть играет роль источника угрозы.

4. Роль маршрутизатора выполняет программный комплекс, установленный на одной из виртуальных машин кластера, с которой также будут считываться данные о трафике и загруженности сети, что позволит проводить более чистый эксперимент.

Структура испытательного стенда представлена на рис.3.

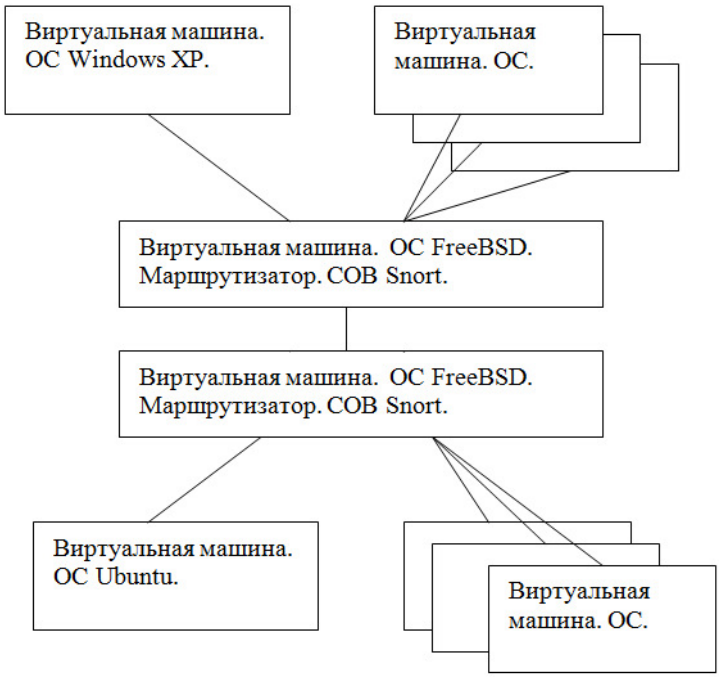

Рис. 3. Структура испытательного стенда

Основные сетевые настройки стенда изображены на рис.4.

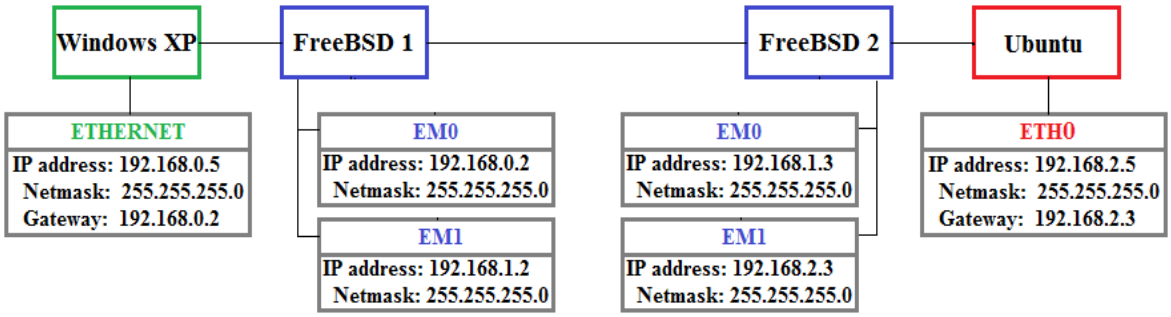

Рис. 4. Основные сетевые настройки стенда

Настройки ОС Windows XP представлены на рис.5.

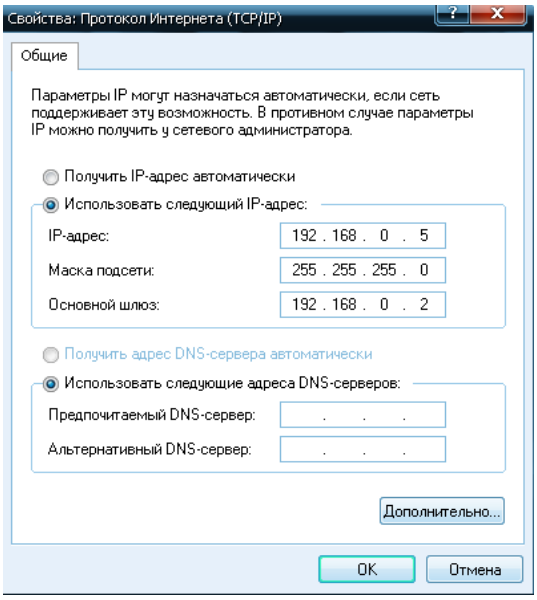

Рис. 5. Сетевые настройки Windows XP

Настройки ОС FreeBSD 1 представлены на рис.6.

```
# Файл /etc/rc.conf
# Назначение IP адресов для интерфейсов em0 и em1
ifconfig_em0=”inet 192.168.0.2 netmask 255.255.255.0”
ifconfig_em1=”inet 192.168.1.2 netmask 255.255.255.0”
# Статический маршрут в сеть с Ubuntu через маршрутизатор FreeBSD 2
static_routes=”net”
route_net=”-net 192.168.2.0/24 192.168.1.3”
# Включение маршрутизации
gateway_enable=”YES”
```

Рис. 6. Сетевые настройки FreeBSD 1

Настройки FreeBSD 2 представлены на рис.7.

```
# Файл /etc/rc.conf
# Назначение IP адресов для интерфейсов em0 и em1
ifconfig_em0=”inet 192.168.1.3 netmask 255.255.255.0”
ifconfig_em1=”inet 192.168.2.3 netmask 255.255.255.0”
# Статический маршрут в сеть с Windows XP через маршрутизатор FreeBSD 1
static_routes=”net”
route_net=”-net 192.168.0.0/24 192.168.1.2”
# Включение маршрутизации
gateway_enable=”YES”
```

Рис. 7. Сетевые настройки FreeBSD 2

Настройки ОС Ubuntu представлены на рис.8.

```
# Файл /etc/network/interfaces
auto eth0
iface eth0 inet static
# IP адрес
address 192.168.2.5
# Маска подсети
netmask 255.255.255.0
# Маршрутизатор по умолчанию
gateway 192.168.2.3
```

Рис. 8. Сетевые настройки Ubuntu

Тестирование работоспособности указанной конфигурации стенда (сетевого взаимодействия виртуальных машин) выполняется с использованием команды *ping* (рис.9).

```
ubuntu@linux:~$ ifconfig eth0
eth0   Link encap:Ethernet HWaddr 08:00:27:cc:ab:13
       inet addr:192.168.2.5 Bcast:192.168.2.255 Mask:255.255.255.0
       inet6 addr: fe80::a00:27ff:fecc:ab13/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:21 errors:0 dropped:0 overruns:0 frame:0
       TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:1374 (1.3 KB) TX bytes:9746 (9.7 KB)

ubuntu@linux:~$ ping 192.168.0.5
PING 192.168.0.5 (192.168.0.5) 56(84) bytes of data.
64 bytes from 192.168.0.5: icmp_req=1 ttl=126 time=0.690 ms
64 bytes from 192.168.0.5: icmp_req=2 ttl=126 time=0.606 ms
64 bytes from 192.168.0.5: icmp_req=3 ttl=126 time=0.653 ms
^C
--- 192.168.0.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.606/0.649/0.690/0.045 ms
ubuntu@linux:~$
```

Рис. 9,а. Тестирование сетевого взаимодействия виртуальных машин (Ubuntu)

```
C:\Users\Admin>ipconfig

Настройка протокола IP для Windows

Подключение по локальной сети - Ethernet адаптер:

       DNS-суффикс этого подключения . . :
       IP-адрес  . . . . . . . . . . . . : 192.168.0.5
       Маска подсети . . . . . . . . . . : 255.255.255.0
       Основной шлюз . . . . . . . . . . : 192.168.0.2

C:\Users\Admin>ping 192.168.2.5

Обмен пакетами с 192.168.2.5 по 32 байт:
Ответ от 192.168.2.5: число байт=32 время=1мс TTL=62
Ответ от 192.168.2.5: число байт=32 время<1мс TTL=62
Ответ от 192.168.2.5: число байт=32 время<1мс TTL=62
Ответ от 192.168.2.5: число байт=32 время<1мс TTL=62

Статистика Ping для 192.168.2.5:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 <0% потерь>,
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек
C:\Users\Admin>
```

Рис. 9,б. Тестирование сетевого взаимодействия виртуальных машин (Windows XP*)*

Краткие выводы.

Указанные настройки обеспечивают сетевое взаимодействие между виртуальными машинами.

Указанные настройки могут быть использованы для проведения удаленного тестирования защитных механизмов операционных систем виртуальных машин.

Список литературы

1. 1.Lincoln Laboratory ID Evaluation Website, MIT, URL. http://www.ll.mit.edu/IST/ideval/index.html (дата обращения:15.05.2013г.).
2. Lippmann, Richard et al. Evaluating Intrusion Detection Systems: The 1998 DARPA Off-line Intrusion Detection Evaluation. Proceedings of DARPA Information Survivability Conference & Exposition (DISCEX), Hilton Head, South Carolina, 25-27 January 2000. Los Alamitos, CA: IEEE Computer Society, 1999: Vol. 2, 12-26.
3. A. J. Anoprienko, V. S. Mirgorod, Donetsk National Technical University, Virtualization technologies: evolution and application prospects, 2009.