УКД 681.3

# СХЕМА ФОРМИРОВАНИЯ ВИРТУАЛЬНОЙ ЛОКАЛЬНОЙ СЕТИ НА БАЗЕ ОБОРУДОВАНИЯ ЛАБОРАТОРИИ ПО АНАЛИЗУ ЗАЩИТЫ СЕТЕЙ.

**Беда И.А.**
**Научный руководитель — к-т.ф.-м.н., профессор Шитов Ю.А.**
***Сибирский федеральный университет***

Рассмотрим локальную сеть, схема которой приведена на рисунке 1.

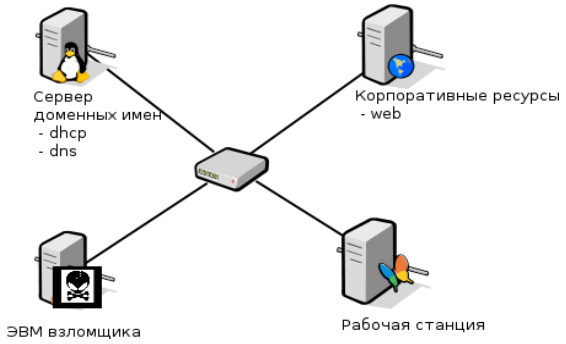


Рис. 1. Схема сети на которой демонстрируется атака

На данной схеме:

сервер доменных имен — ЭВМ под управление операционной системы Linux, сконфигурированная как динамический DNS сервер.

DNS (Domain Name System) - компьютерная распределённая система для получения информации о доменах. Используется для получения IP-адреса по имени ЭВМ. Принцип работы динамического DNS заключается в следующем: сервер по протоколу DHCP предает параметры TCP/IP клиентам, а также запрашивает их доменные имена. Эти доменные имена используются DNS сервером. Таким образом ЭВМ в сети обращаются друг к другу по своим доменным именам.

Корпоративные ресурсы — в качестве таковых ресурсов используется веб-сервер под управление операционной системы Linux.

Рабочая станция — ЭВМ под управление операционной системы Windows XP SP3 с интернет-браузером Internet Explorer 6.

Компьютер взломщика - ЭВМ под управление операционной системы Linux, на которой взломщик имеет права администратора.

Для формирования сети, представленной на рисунке 1, используются ресурсы локальной сети, представленной на рисунке 2, спроектированной и реализованной в лаборатории по анализу защиты сетей на кафедре ПМКБ института космических и информационных технологий (ИКИТ) СФУ. Подробное описание сети приведено в докладе «Проектирование локальной сети для лаборатории по анализу защиты сетей».

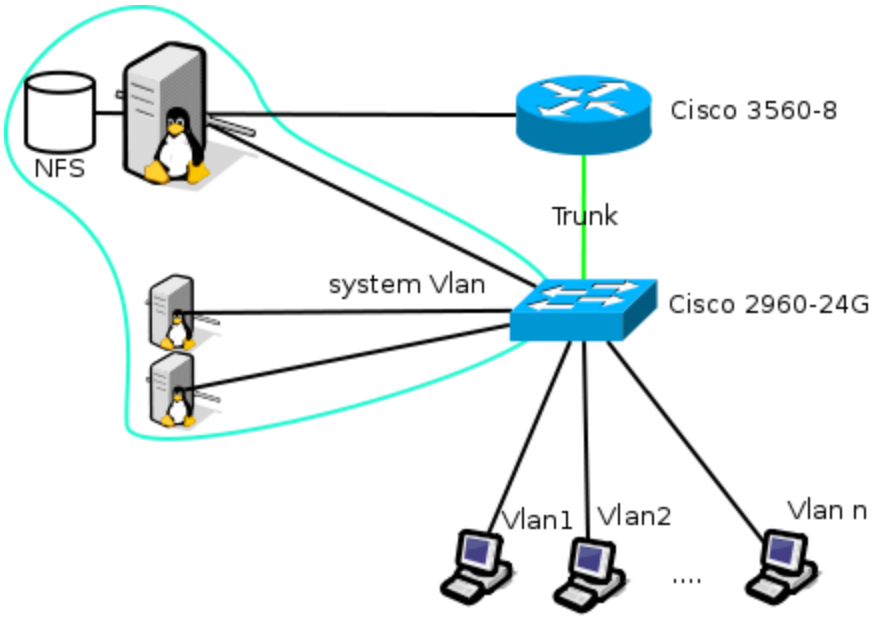


Рис. 2. Локальная сеть лаборатории по анализу защиты сетей

Для формирования локальной сети необходимо: создание виртуальных жестких дисков для виртуальных машин. Создание виртуального жесткого диска представлено в листинге 1.

Листинг 1. Создание виртуального жесткого диска

```
$qemu-kvm create <имя_диска> 10G
```

На жесткие диски для сервера доменных имен, сервера корпоративных ресурсов и ЭВМ взломщика необходимо установить операционную систему Linux, а на жесткий диск рабочей станции установить Windows SP3.

Далее необходимо установить и настроить следующие программы:

- для сервера доменных имен - dhcp-dns сервер dnsmasq;
- для сервера корпоративных ресурсов - веб-сервер lighttpd;
- для ЭВМ взломщика — metasploit framework 3.3, arp-sk.

После этого полученные виртуальные машины необходимо объединить в сеть, для этого используется интерфейс типа «мост». Для создания и управления интерфейсами типа «мост» в операционной системе Linux предназначен пакет программ bridge-utils.

К мосту подключаются TAP интерфейсы, через которые Ethernet пакеты передаются виртуальным сетевым картам. В терминологии компьютерных сетей TAP — виртуальный сетевой драйвер ядра системы. TAP эмулирует Ethernet устройство и работает на канальном уровне модели OSI, оперируя кадрами Ethernet.

Для создания и управления интерфейсами типа TAP в операционной системе Linux предназначена утилита tunctl из пакета программ User Mode Linux Utilities.

Для того, чтобы трафик виртуальной сети не попадал в реальную сеть на интерфейсе «мосте», необходимо отключить STP протокол и выделить для сети отдельный VLAN.

Spanning Tree Protocol — сетевой протокол, работающий на втором уровне модели OSI. Основан на алгоритме STA Spanning Tree algorithm (алгоритм покрывающего дерева). Основной задачей STP является приведение сети Ethernet с множественными связями к древовидной топологии, исключающей циклы пакетов.

В случае, если STP протокол включен, то Ethernet кадры из одной виртуальной сети будут попадать в другую виртуальную сеть, если в обеих сетях есть ЭВМ с одинаковым IP адресом.

Для автоматизации запуска виртуальных машин используется следующий bash-скрипт, приведенный в листинге 2. Скриптовый язык — язык программирования, разработанный для записи «сценариев», последовательностей операций, которые пользователь может выполнять на компьютере. Bash - одна из наиболее популярных современных разновидностей командной оболочки UNIX. Bash позволяет разрабатывать скрипты. Для запуска bash-скрипта необходимо передать интерпретатору bash путь до файла скрипта. В общем случае запуск скрипта будет выглядеть следующим образом: bash /путь/до/файла.

Листинг 2. Скрипт для запуска виртуальной инфраструктуры

```
 1  brctl addbr br0
 2  ifconfig br0 0.0.0.0  up
 3  brctl stp br0 off
 4  tunctl -b -u root -t dns.e0
 5  tunctl -b -u root -t web.e0
 6  tunctl -b -u root -t hack.e0
 7  tunctl -b -u root -t win.e0
 8  brctl addif br0 web.e0
 9  ifconfig web.e0 0.0.0.0 up
10 brctl addif br0 win.e0
11 ifconfig win.e0 0.0.0.0 up
12 brctl addif br0 hack.e0
13 ifconfig hack.e0 0.0.0.0 up
14 brctl addif br0 dns.e0
15 ifconfig dns.e0 0.0.0.0 up
16 qemu-kvm -hda dnsdhcp.img  -m 512 -daemonize\
17 -net nic,macaddr=00:00:C6:00:6C:21,vlan=10\
18 -net tap,ifname=dns.e0,script=no,vlan=10
19 qemu-kvm -hda web.img -m 512 -daemonize\
20 -net nic,macaddr=00:00:C6:00:6C:11,vlan=10\
21 -net tap,ifname=web.e0,script=no,vlan=10
22 qemu-kvm -hda hack.img -m 512 -vnc :0 -daemonize\
23 -net nic,macaddr=00:01:C6:00:6C:01,vlan=10\
24 -net tap,ifname=hack.e0,script=no,vlan=10
25 qemu-kvm -hda win.img -m 512 -daemonize -vnc :1\
26 -net nic,macaddr=00:01:C6:E6:6C:02,vlan=10\
27 -net tap,ifname=win.e0,script=no,vlan=10
```

Рассмотрим, что делает этот скрипт.

Строка 1 — создаем интерфейс «br0» типа «мост».

Строка 2 — настраиваем интерфейс. Так как виртуальная инфраструктура изолирована и не должна быть связана с реальной сетью, то мы устанавливаем ip адрес интерфейса «br0» в «0.0.0.0» .

Строка 3 — отключаем STP протокол на интерфейсе «br0».

Строки с 4 по 7 — создаем туннельные интерфейсы  для виртуальных сетевых карт.

Строки с 8 по 15 — настраиваем туннельные интерфейсы «win.e0», «web.e0», «hack.e0», «dns.e0». Командой «brctl addif br0» подключаем туннельный интерфейс к интерфейсу «br0». Поле такого подключения интерфейс «br0» будет пересылать пакеты

от одного туннельного интерфейса к другому. Для адресации используются MAC адреса виртуальных сетевых карт.
Строка 16 — запускаем виртуальный dhcp-dns сервер.
Строка 22 — запускаем виртуальный веб вервер.
Строка 28 — запускаем ЭВМ взломщика.
Строка 35 — запускаем рабочую станцию.
Рассмотрим параметры, с которыми запускаются виртуальные машины.

Через ключ «-hda» передается путь до файла виртуального жесткого диска. «-m» отвечает за объем оперативной памяти виртуальной машины. «-net,nic» создает виртуальную сетевую карту и подключает к указанному VLAN (по умолчанию 0) параметр «vlan=», а также устанавливает MAC-адрес, параметр «macaddr=». «-net,tap» подключает виртуальную сетевую карту к tap интерфейсу, параметр «vlan=» указывает на используемый VLAN (по умолчанию 0), через параметр «ifname=» передается имя интерфейса, «script=» указывает на файл со скриптом начальной инициализации туннельного интерфейса, так как туннельные интерфейсы уже инициализированы и выполнять скрипт не нужно, то используется значение «no».

Ключ «-vnc» отвечает за параметры vnc сервера, через который пользователь получит доступ к виртуальной машине. VNC (Virtual Network Computing) — система удалённого доступа к рабочему столу компьютера, использующая протокол RFB (Remote FrameBuffer). Управление осуществляется путём передачи нажатий клавиш на клавиатуре и движений мыши с одного компьютера на другой и ретрансляции содержимого экрана через компьютерную сеть. Так как для выполнения лабораторной работы необходим доступ к ЭВМ взломщика и рабочей станции, то для запуска используется ключ «-vnc». Параметры «:0» и «:1» отвечают за номер виртуального дисплея. Таким образом, через виртуальный дисплей под номером 0 осуществляется доступ к ЭВМ взломщика, а через виртуальный дисплей под номером 1 — к рабочей станции. После запуска данного скрипта на сервере будет запущена виртуальная инфраструктура для выполнения лабораторной работы.