Индивидуальный проект. Этап 2

Установка DVWA

Буллер Т.А.

20 февраля 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Буллер Татьяна Александровна
- студент направления Бизнес-информатика
- Российский университет дружбы народов

Вводная часть

Объект и предмет исследования

- Веб-приложение DVWA в составе Metasploitable
- Виртуальная машина Kali Linux
- Среда виртуализации VirtualBox

Цели и задачи

- Приобретение практических навыков создания виртуальной машины и запуска веб-сервера.

Материалы и методы

- Файлы установки Metasploitable для VMware
- Среда виртуализации VirtualBox
- Виртуальная машина Kali Linux

Ход работы

Ход работы

Установка DVWA в данной работе будет рассмотрена в комплексе с созданием машины Metasploitable. Metasploitable - намеренно уязвимая машина, содержащая внутри себя такие веб-приложения, как DVWA, WebDAV и Mutillidae. DVWA - намеренно уязвимое веб-приложение, написанное на PHP и MySQL. Изначально Metasploitable создавался в расчете на совместимость с VMware, но VirtualBox также поддерживает формат виртуальных дисков .vmdk, с которого машина может быть запущена. Для этого добавим диск Metasploitable при выборе диска для машины.

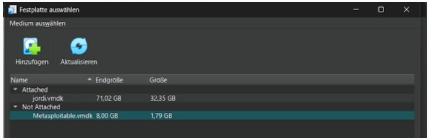

Рис. 1: Добавление виртуального диска

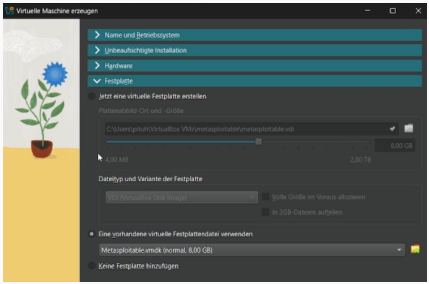

Рис. 2: Настройки диска

Metasploitable не предназначен для использования в качестве полностью рабочей машины, ресурсов ему оставим по минимуму: 2 CPU и 512 МБ оперативной памяти.

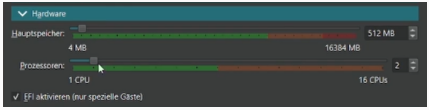

Рис. 3: Настройки ресурсов системы

Данные о системе в данном случае придется настраивать вручную, так как файл образа не используется. Здесь выбираем имя, место хранения, тип ОС - Линукс, подтип - другой, версия - x64.

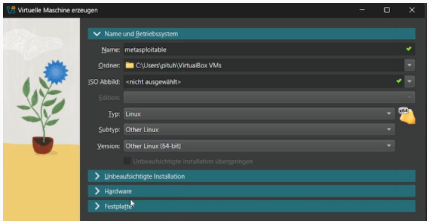

Рис. 4: Основные настройки

Для того, чтобы машины видели друг друга в локальной сети, подключим Metasploitable в тот же сегмент NAT, куда уже подключена основная виртуальная машина.

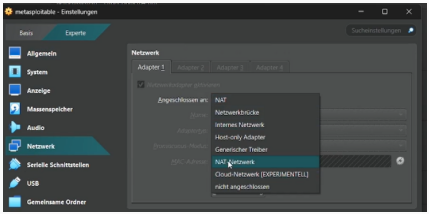

Рис. 5: Настройки сети

Машина запускается самостоятельно без дополнительных настроек и установки. Логин и пароль по умолчанию совпадают: msfadmin:msfadmin.

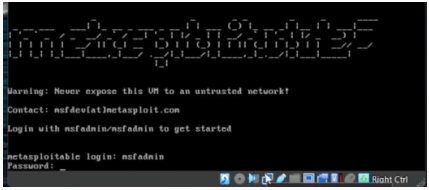

Рис. 6: Запуск Metasploitable

Для проверки правильности настройки просмотрим адрес сетевого интерфейса машины (должен быть в сегменте 192.168.6.0/24) и попробуем пропинговать рабочую машину с адресом в той же сети 192.168.6.12. Пинг проходит, машины друг друга видят - можно продолжать работу.

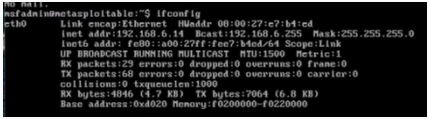

Рис. 7: Сетевой интерфейс Metasploitable

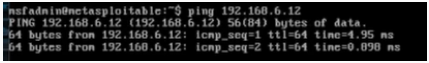

Рис. 8: Пинг рабочей машины

На рабочей машине в адресную строку браузера введем адрес Metasploitable: 192.168.6.14. Попадаем на основную страницу, где видим предупреждение никогда не выводить эту машину в сети, которым не доверяем, контакты разработчиков и дефолтные логин и пароль; ниже - ссылки на сервисы, которые встроены в Metasploitable.

Рис. 9: Основная страница Metasploitable

Перейдем на страницу DVWA. Там нас встречает простая форма логина, ниже - логин и пароль по умолчанию (admin:password).

Рис. 10: login.php DVWA

Использовав эти данные, мы успешно входим в систему. На первой странице - дисклеймер, предупреждение и общие инструкции. В меню 4 части: основная информация, страницы уязвимостей разных типов, безопасность и информация о машине, выход из системы.

Рис. 11: Корневая страница DVWA

Типы уязвимостей будут рассмотрены по ходу работы над проектом далее. Интересно взглянуть на страницу безопасности системы: тут можно выбрать уровень “сложности” машины. По умолчанию - низкий, доступны также средний, высокий и “невозможный”. Последний должен быть примером идеального написания кода.

Рис. 12: Настройки безопасности

Полезным для исследователя является также файл phpinfo, содержащий конфигурацию php и некоторые данные о системе.

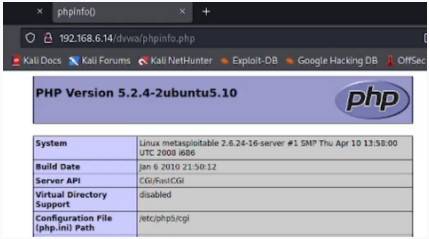

Рис. 13: phpinfo

Ход работы

DVWA можно запустить и не используя для этого дополнительную машину, на локальном хосте. Для этого необходимо будет скачать файлы конфигурации и запустить веб-сервер apache.

Выводы

Выводы

Были приобретены практические навыки создания виртуальной машины по виртуальному диску и запуска веб-сервера.