ЛАБОРАТОРНАЯ РАБОТА №5.

Свидиров Кирилл,11-902

04.05.2022

Содержание

1 Общая информация

- Работу выполнил Свидиров Кирилл Андреевич, 11-902 группа.
- Название лабораторной работы – “ЛАБОРАТОРНАЯ РАБОТА №5. СКАНЕР УЯЗВИМОСТЕЙ NESSUS”.

2 Постановка задачи

2.1 Суть задания

С помощью NESSUS сканера просканировать виртуальную машину Metasploitable на уязвимости.

2.2 Цель упражнения

Научиться использовать сканер NESSUS и прочитать подробную информацию об уязвимостях, которые мы использовали ранее.

2.3 Используемые средства

- Vmware Workstation 16 Player - для запуска виртуальной машины с уязвимым образом Linux – Metasploitable.
- Metasploitable – устаревший и уязвимый образ Linux. Используется, чтобы свободно изучать существующие уязвимости операционной системы.
- Kali Linux – образ Linux, с которого будут совершаться атаки на Metasploitable.
- NESSUS - ПО для сканирования и выявленяи уязвимостей устройства.

3 Исходное состояние

Образ Metasploitable с изменёнными репозиториями. В процессе выполнения лабораторной работы значительных изменений не будет.
Образ Kali. В процессе выполнения лабораторной работы будет:

- Установлен NESSUS

4 Выполнение задания

4.1 Загрузка виртуальной машины Metasploitable

✓ Предварительно был установлен Vmware Workstation 16 Player.

✓ Была успешно загружена машина Metasploitable, используемая в предыдущих работах.

4.2 Загрузка виртуальной машины Kali Linux

✓ Была успешно загружена машина Kali, используемая в предыдущих работах.

4.3 Установка Nessus

4.3.1 Скачивание установочного пакета

✓ На Kali был открыт браузер Explorer

✓ Был совершён переход по следующей ссылке

✓ С сайта был получен установочный пакет для Kali

✓ С помощью команыд [ls -l] в папке /home/kali/Downloads я убедился в успешном получении установочного пакета

4.3.2 Установка и запуск

✓ С помощью команды [dpkg -i Nessus-10.1.2-debian6_amd64.deb] сканер был установлен

✓ С помощью команды [/bin/systerctl start nessusd.service] сканер был запущен

✓ По ссылке https://kali:8834/ было запущено веб-приложение сканера

4.3.3 Регистрация сканера

✓ Прямо в веб-приложении сканера была проведена регистрация, получение активационного ключа по имени, фамилии и почте, ввод ключа и создание логина - пароля.

4.4 Сканирование Metasploitable

4.4.1 Подготовка к работе

(!) Перезапуск машины не осуществлялся, т.к. обе машины прекрасно видят друг-друга с NAT настройкой.

4.4.2 Выполнение сканирования

✓ В веб-приложении сканера была нажата кнопка "New Scan"

✓ Был выбран тип сканера "Advanced Scan"

✓ Скан получил имя "Metasploitable – Internal – Свидиров Кирилл, 11-902"и цель сканирования - 192.168.33.128 (адрес Metasploitable)

- ✓ Полученый шаблон сканера был запущен
- ✓ После окончания сканирования в результатах была найдена уязвимость из лабораторной работы №3 - Samba Badlock Vulnerability.

4.5 Сохранение отчета

- ✓ В папке "Lab 5 Report"лежат необходимые отчёты в форматах html и pdf