

Министерство образования Республики Беларусь
Учреждение образования
«Гомельский государственный университет им. Франциска Скорины»

Отчёт по лабораторной работе №6
«Идентификация уязвимостей на основе тестов»

Выполнил:
Студент группы МС-42
Созинов Л.В.
Проверил:
Грищенко В.В.

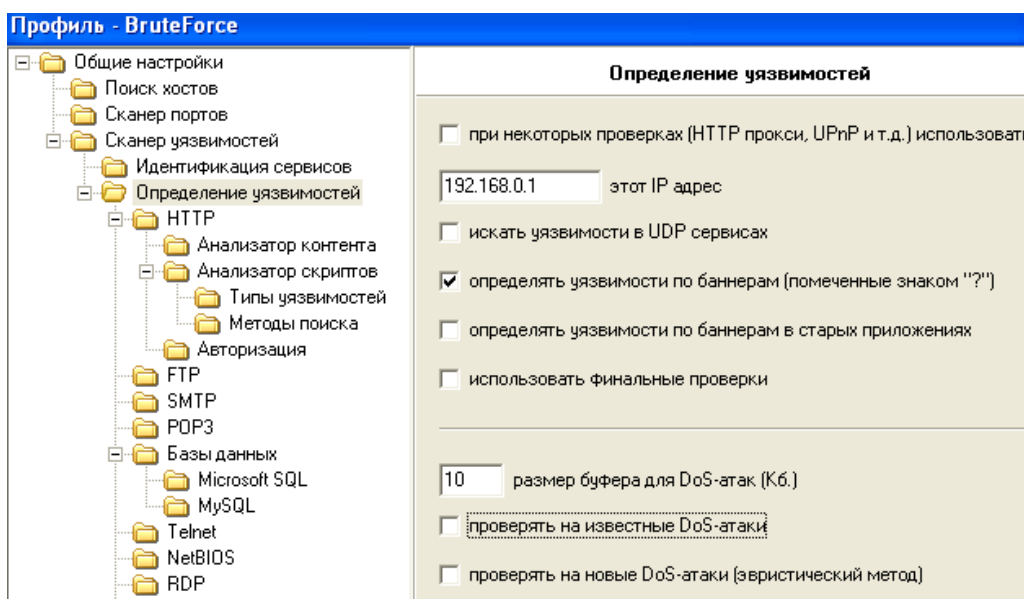
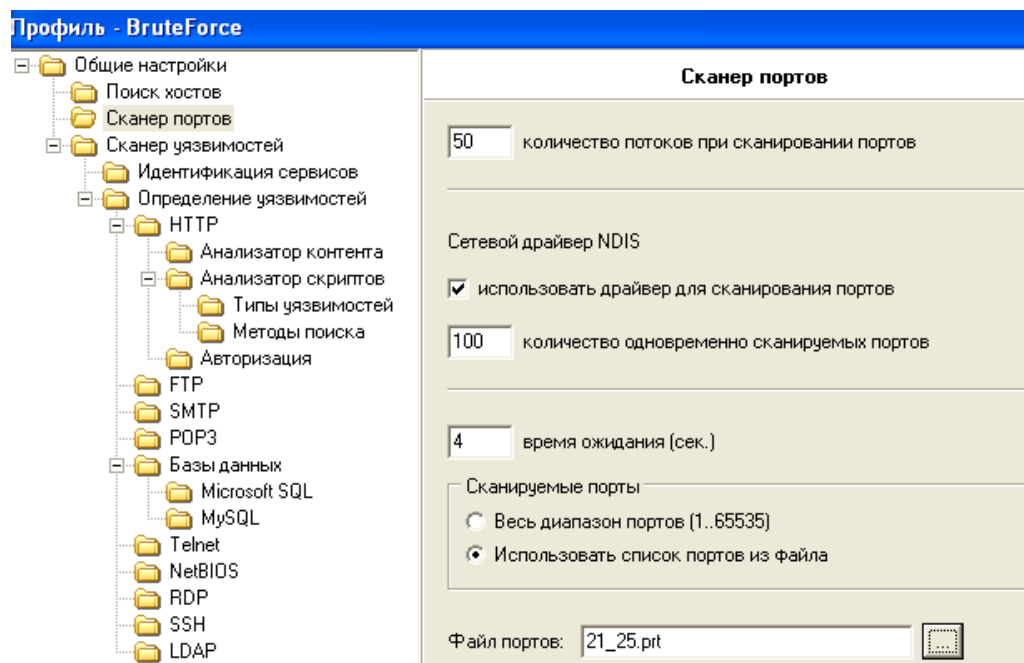
Лабораторная работа №6

Идентификация уязвимостей на основе тестов

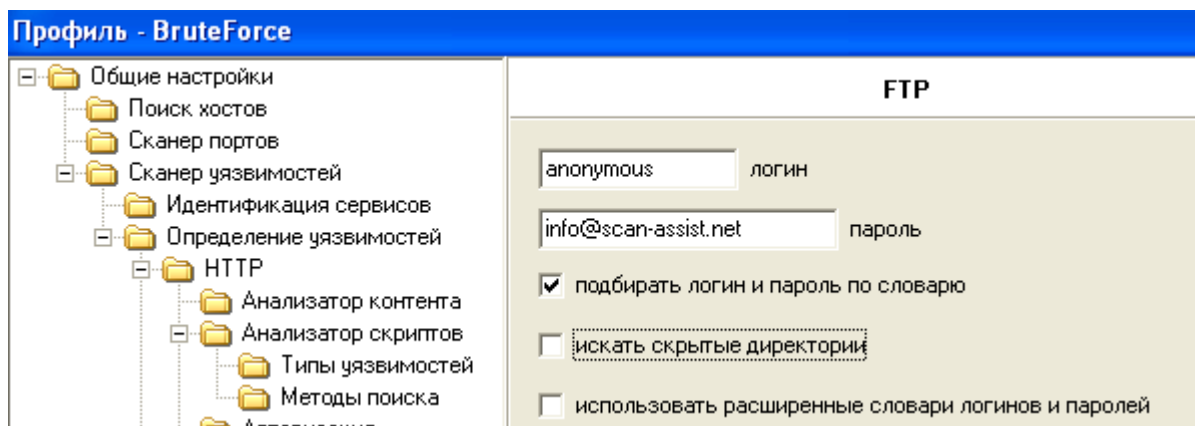
Цель работы: Обучение методам и средствам идентификации уязвимостей на основе тестов.

Ход работы

1. Создадим новый профиль сканирования с именем «BruteForce». Перечень сканируемых портов ограничим портами служб FTP (21) и SMTP (25). Отключим сканирование служб UDP, в секции «Определение уязвимостей» отключим опции «Использовать финальные проверки», «Проверять на известные DoS-атаки», «Проверять на новые DoS-атаки».



2. В секции «Сканер уязвимостей» – «Определение уязвимостей» – «FTP» отключим опцию «Искать скрытые директории». Включим опцию «Подбирать учётные записи», выберем ранее созданные словари логинов и паролей. Сохраним профиль сканирования.



3. Создадим новую задачу «Подбор паролей», выбрав созданный ранее профиль сканирования «BruteForce». Выполним сканирование сервера. Проанализируем результаты. Убедимся в подборе пароля к службам FTP и SMTP.



Информация

Имя хоста (полученное при обратном DNS запросе):	computer.domain
Время отклика:	< 1 мсек
TTL:	128

Параметры сканирования

Начало сканирования:	11:14:55 07.12.2022
Время сканирования:	00:00:35
Версия:	7.7 Demo Build 3100
Профиль:	BruteForce.prf

4. Создадим профиль сканирования «DoS». В список сканируемых портов добавим TCP порты 21 и 25. Отключим сканирование служб UDP. Включим опции «Искать уязвимости». В секции «Определение уязвимостей» включим опции «Использовать финальные проверки», «Проверять на известные DoS-атаки». Отключим опцию «Подбирать учетные записи».

Профиль - DoS

Общие настройки

Поиск хостов

Сканер портов

Сканер уязвимостей

Идентификация сервисов

Определение уязвимостей

HTTP

Анализатор контента

Анализатор скриптов

Типы уязвимостей

Методы поиска

Авторизация

FTP

SMTP

POP3

Базы данных

Microsoft SQL

MySQL

Telnet

NetBIOS

RDP

SSH

LDAP

Сканер портов

50

количество потоков при сканировании портов

Сетевой драйвер NDIS

☒ использовать драйвер для сканирования портов

100

количество одновременно сканируемых портов

4

время ожидания (сек.)

Сканируемые порты

☐ Весь диапазон портов (1..65535)

☒ Использовать список портов из файла

Файл портов:

21_25.prt

Профиль - DoS

Общие настройки

Поиск хостов

Сканер портов

Сканер уязвимостей

Идентификация сервисов

Определение уязвимостей

HTTP

Анализатор контента

Анализатор скриптов

Типы уязвимостей

Методы поиска

Авторизация

FTP

SMTP

POP3

Базы данных

Microsoft SQL

MySQL

Telnet

NetBIOS

RDP

SSH

LDAP

Определение уязвимостей

☐ при некоторых проверках (HTTP прокси, UPnP и т.д.) использовать

192.168.0.1

этот IP адрес

☐ искать уязвимости в UDP сервисах

☒ определять уязвимости по баннерам (помеченные знаком "?")

☐ определять уязвимости по баннерам в старых приложениях

☒ использовать финальные проверки

10

размер буфера для DoS-атак (Кб.)

☒ проверять на известные DoS-атаки

☒ проверять на новые DoS-атаки (эвристический метод)

5. Создадим задачу «Финальные проверки», используя профиль «DoS». Выполним сканирование.


Хост
172.16.0.1

Информация

Имя хоста (полученное при обратном DNS запросе):	computer.domain
Время отклика:	< 1 мсек
TTL:	128

Параметры сканирования

Начало сканирования:	11:21:24 07.12.2022
Время сканирования:	00:01:24
Версия:	7.7 Demo Build 3100
Профиль:	DoS.prf