

Гомельский Государственный Университет
им. Ф. Скорины

Лабораторная работа №6.
Идентификация уязвимостей на основе тестов

Проверил:

Грищенко В.В.

Студент МС – 42:

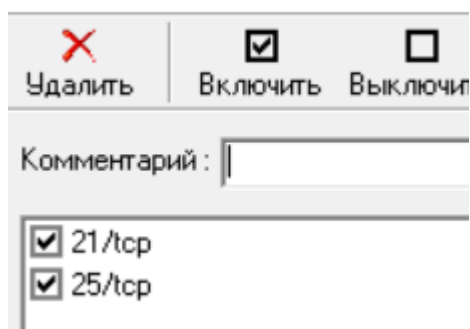
Черненко А.В.

Цель работы: Целью лабораторной работы является обучение методам и средствам идентификации уязвимостей на основе тестов.

Постановка задачи: выполнить идентификацию уязвимостей и подбор учетных записей с использованием сканера безопасности XSpider.

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

Новый файл портов

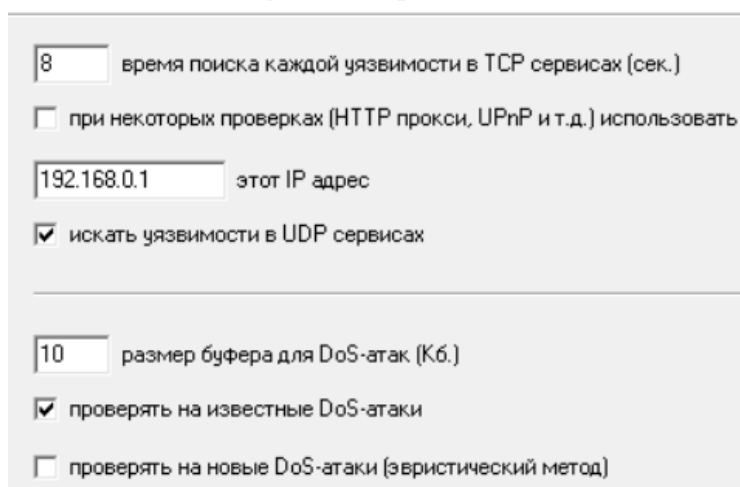


Удалить Включить Выключить

Комментарий :

☒ 21/tcp
☒ 25/tcp

Определение уязвимостей



8 время поиска каждой уязвимости в TCP сервисах (сек.)

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

192.168.0.1 этот IP адрес

☒ искать уязвимости в UDP сервисах

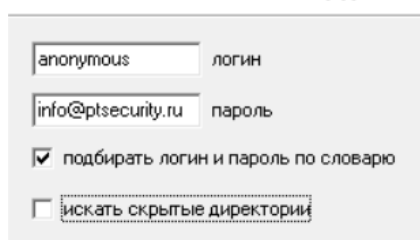
10 размер буфера для DoS-атак (Кб.)

☒ проверять на известные DoS-атаки

☐ проверять на новые DoS-атаки (эвристический метод)

Шаг 2. В секции «Сканер уязвимостей» – «Определение уязвимостей» – «FTP» отключить опцию «Искать скрытые директории». Включить опцию «Подбирать учётные записи», выбрать ранее созданные словари логинов и паролей. Сохранить профиль сканирования.

FTP



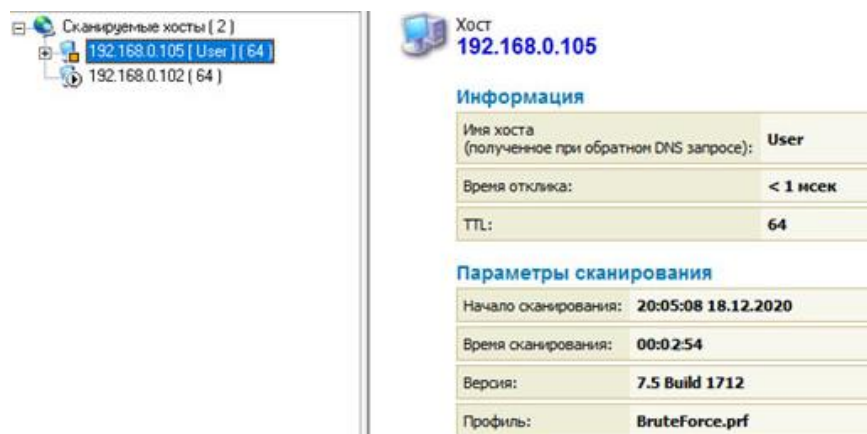
anonymous login

info@ptsecurity.ru пароль

☒ подбирать логин и пароль по словарю

☐ искать скрытые директории

Шаг 3. Создать новую задачу «Подбор паролей», выбрав созданный ранее профиль сканирования «BruteForce». Выполнить сканирование сервера S2. Проанализировать результаты. Убедиться в подборе пароля к службам FTP и SMTP.



The screenshot shows the Nmap interface. On the left, a tree view under 'Сканируемые хосты [2]' lists '192.168.0.105 [User] [64]' and '192.168.0.102 [64]'. The main panel displays details for host '192.168.0.105'.

Хост
192.168.0.105

Информация

Имя хоста (полученное при обратном DNS запросе):	User
Время отклика:	< 1 мсек
TTL:	64

Параметры сканирования

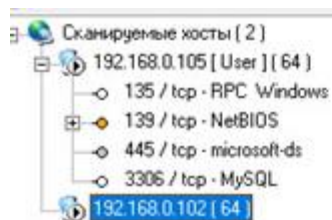
Начало сканирования:	20:05:08 18.12.2020
Время сканирования:	00:02:54
Версия:	7.5 Build 1712
Профиль:	BruteForce.nrf

Шаг 4. Создать профиль сканирования «DoS». В список сканируемых портов добавить TCP порты 21 и 25. Отключить сканирование служб UDP. Включить опции «Искать уязвимости». В секции «Определение уязвимостей» включить опции «Использовать финальные проверки», «Проверять на известные DoS-атаки». Отключить опцию «Подбирать учетные записи».

Определение уязвимостей

<input type="text" value="8"/>	время поиска каждой уязвимости в TCP сервисах (сек.)
<input type="checkbox"/>	при некоторых проверках (HTTP прокси, UPnP и т.д.) использовать
<input type="text" value="192.168.0.1"/>	этот IP адрес
<input type="checkbox"/>	искать уязвимости в UDP сервисах
<hr/>	
<input type="text" value="10"/>	размер буфера для DoS-атак (Кб.)
<input checked="" type="checkbox"/>	проверять на известные DoS-атаки
<input checked="" type="checkbox"/>	проверять на новые DoS-атаки (эвристический метод)

Шаг 5. Создать задачу «Финальные проверки», используя профиль «DoS». Выполнить сканирование.



Хост
192.168.0.102

Информация

Время отклика: **3 мсек**

TTL: **64**

Параметры сканирования

Начало сканирования: **20:05:08 18.12.2020**

Версия: **7.5 Build 1712**

Профиль: **BruteForce.prf**