МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования   
«Гомельский государственный университет имени Франциска Скорины»

Факультет физики и информационных технологий

Кафедра общей физики

ОТЧЕТ по лабораторной работе №3

по теме «Идентификация служб и приложений»

Выполнил:

Студент группы МС-32 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Черкас Е.О.

(подпись)

Проверил:

Старший преподаватель \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Грищенко В.В.

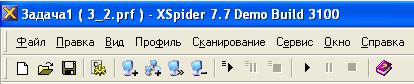
(подпись)

Гомель 2022

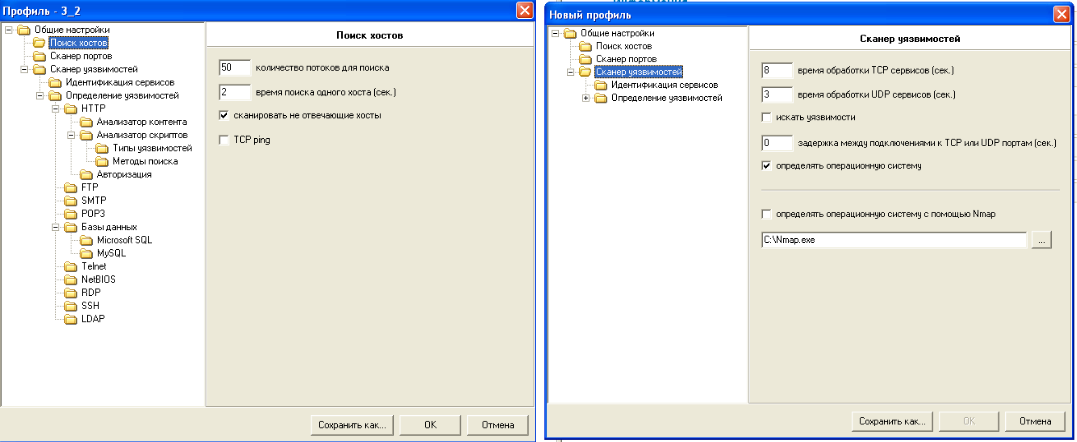
**Лабораторная работа №3**

***Цель работы:*** обучение методам и средствам идентификации служб и приложений, соответствующих открытым сетевым портам анализируемой КС.

**Шаг 1.** На узле TWS2 прейдем в консоль XSpider. Создадим новый профиль сканирования.



**Шаг 2.** На узле TWS2 перейти в консоль XSpider. Создать новый профиль сканирования. Включить опцию ICMP ping, отключить опцию TCP ping, отключить опцию «Сканировать не отвечающие хосты», в секции «Сканер портов» задать параметр «Список портов» 1-200, в секции «Сканер уязвимостей» отключить опцию «Искать уязвимости».

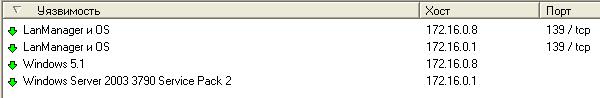


**Шаг 3.** Запустить сканирование служб и приложений сервера S1. Проверить, что службы FTP, SMTP, НТТР и другие найдены и идентифицированы.

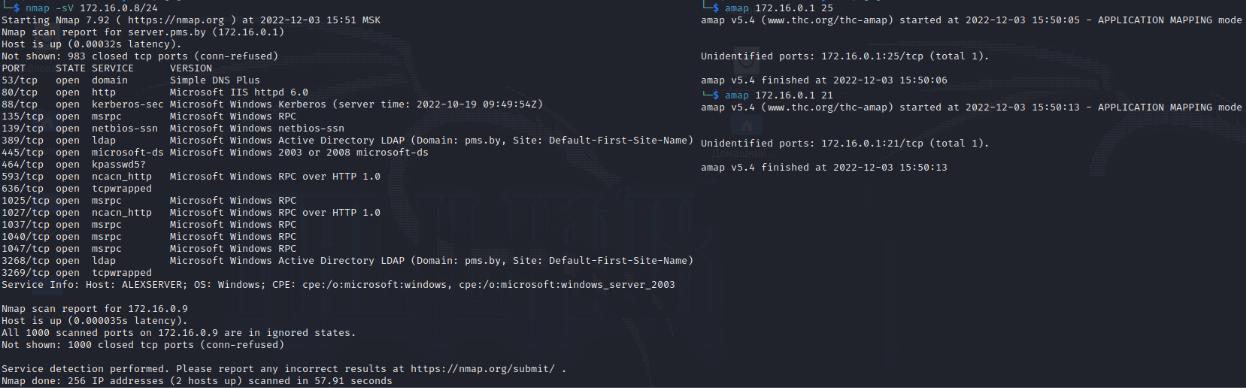




**Шаг 4.** Проверить наличие уязвимостей при сканировании.



**Шаг 5.** На узле TWS1 с помощью сетевых сканеров nmap и amap выполнить идентификацию служб и приложений узлов S1 и S2. Просмотреть трассировки сканирований.



**Вывод:** в ходе лабораторной работы были получены знания о методах и средствах идентификации служб и приложений, соответствующих открытым сетевым портам анализируемой КС.