Министерство образования Республики Беларусь

Учреждение образования

“Гомельский государственный университет им. Франциска Скорины”

Отчёт по лабораторной работе №3

«Идентификация служб и приложений»

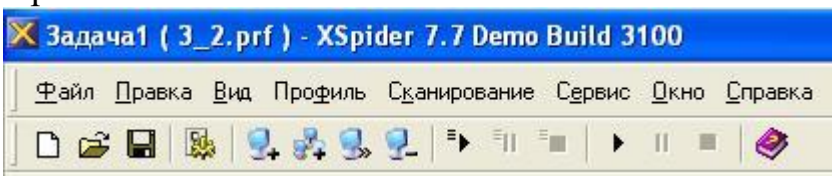
Выполнил:
Студент группы МС-42
Баль П.М.
Проверил: Грищенко В.В.

2022

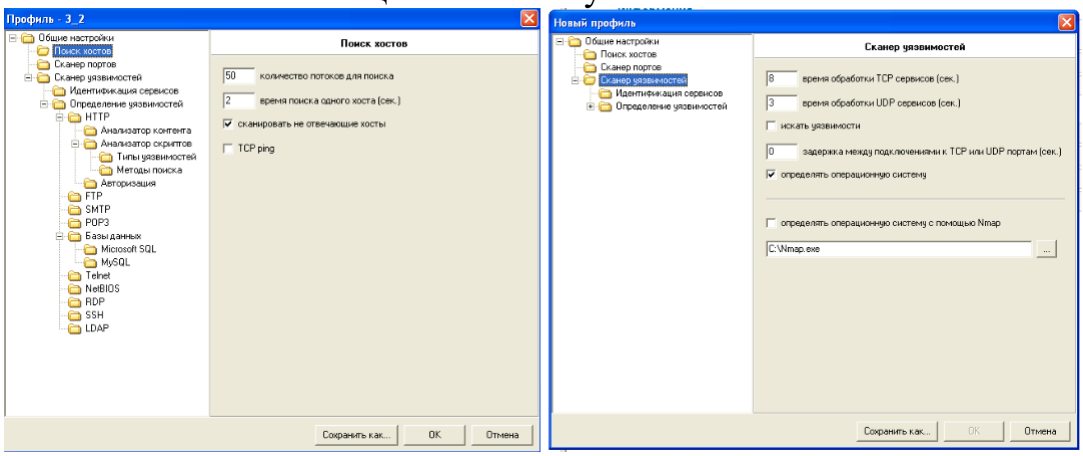
Лабораторная работа №3

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

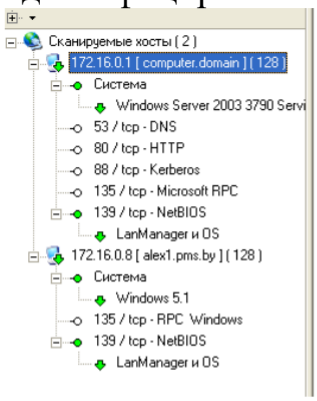
Шаг 1. На узле TWS2 прейдем в консоль XSpider. Создадим новый профиль сканирования.



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, HTTP и другие найдены и идентифицированы.



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:	13:05:54 20.11.2022
Время сканирования:	00:02:05
Версия:	7.7 Demo Build 3100
Профиль:	3_2.prf

Доступна информация
Windows Server 2003 3790 Service Pack 2

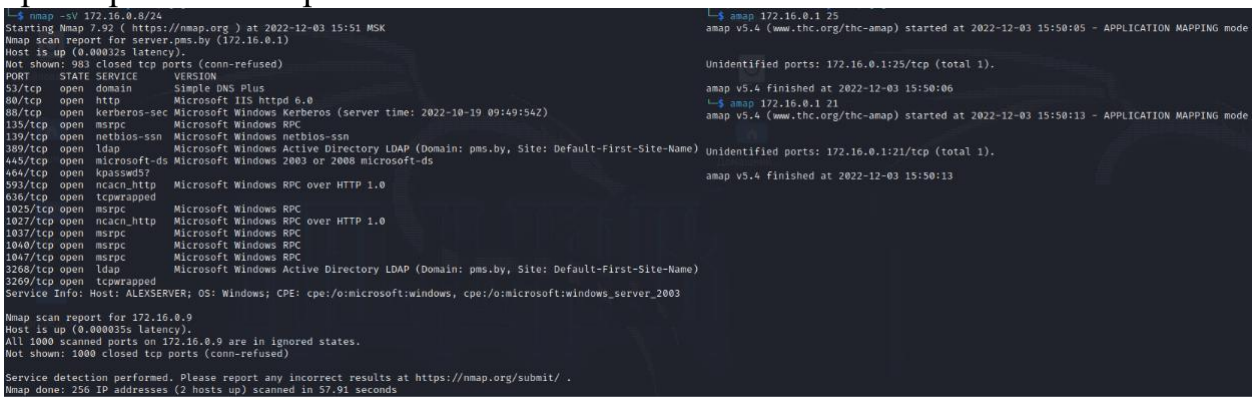
Описание

Вероятная версия операционной системы : Windows Server 2003 3790 Service Pack 2

Шаг 4. Проверить наличие уязвимостей при сканировании.

Уязвимость	Хост	Порт
LanManager и OS	172.16.0.8	139 / tcp
LanManager и OS	172.16.0.1	139 / tcp
Windows 5.1	172.16.0.8	
Windows Server 2003 3790 Service Pack 2	172.16.0.1	

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.