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

Отчёт по лабораторной работе №3
«Идентификация служб и приложений»

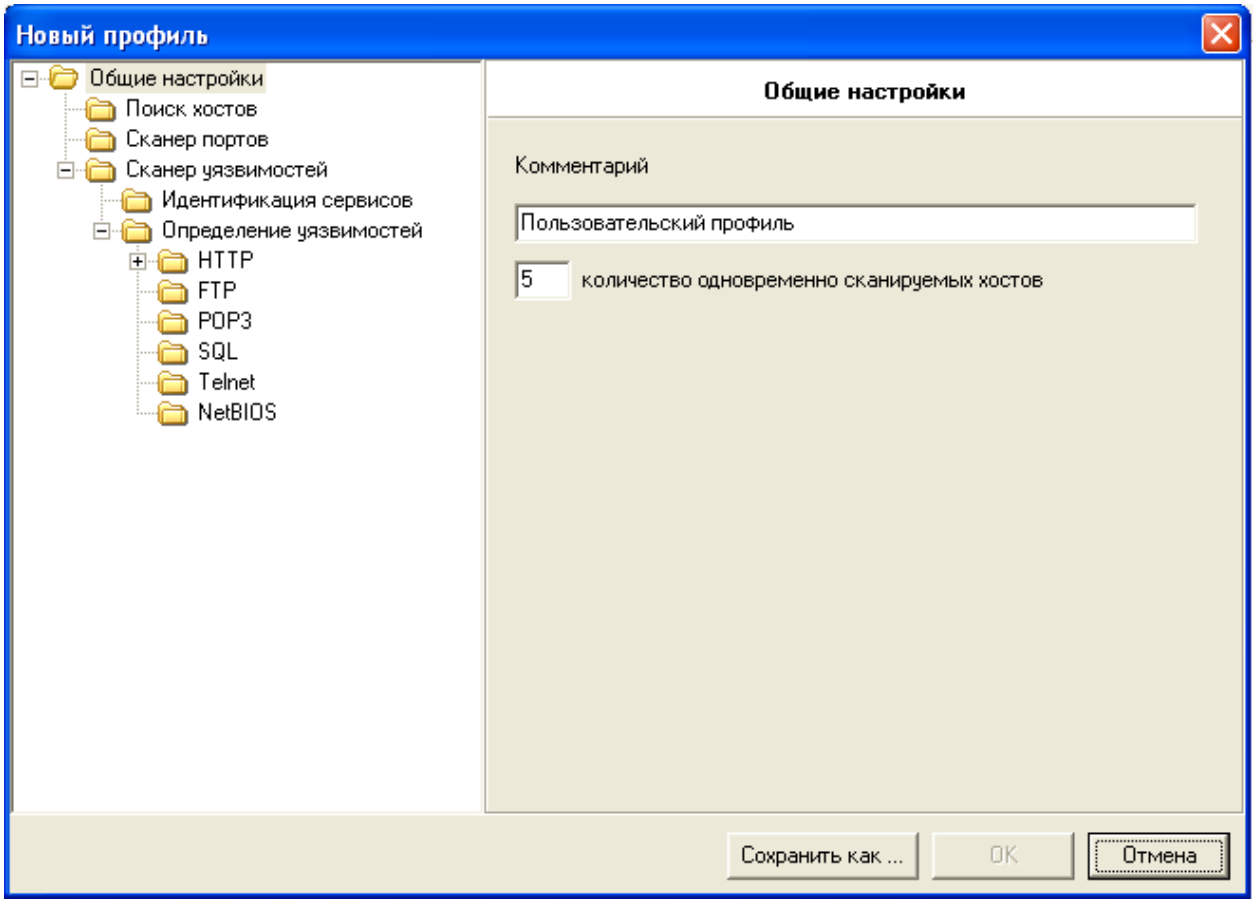
Выполнил студент группы МС-42: Казак И.В.
Проверил:
Старший преподаватель Грищенко В.В.

Гомель 2022

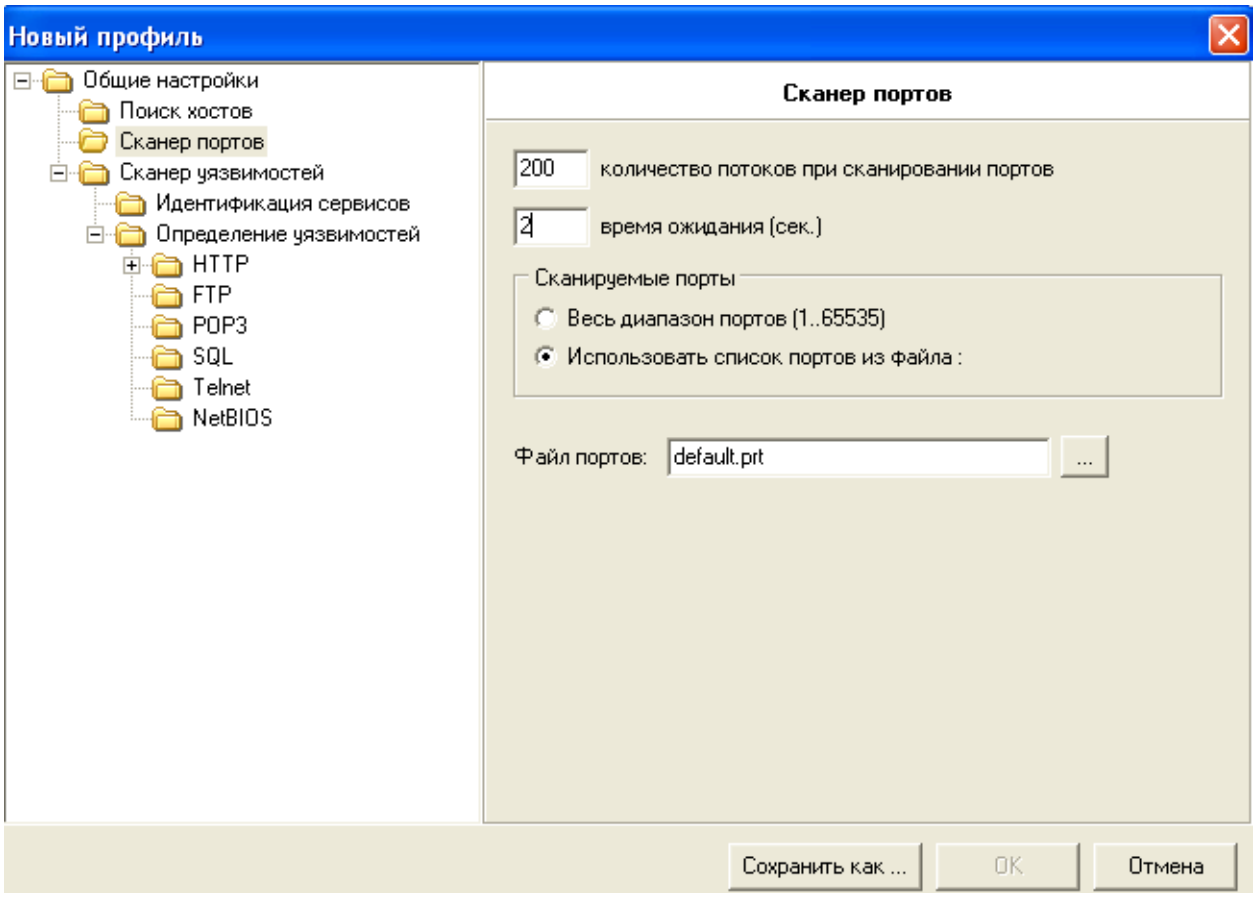
Цель работы: обучение методам и средствам идентификации служб и приложений, соответствующих открытым сетевым портам анализируемой КС.

Ход работы.

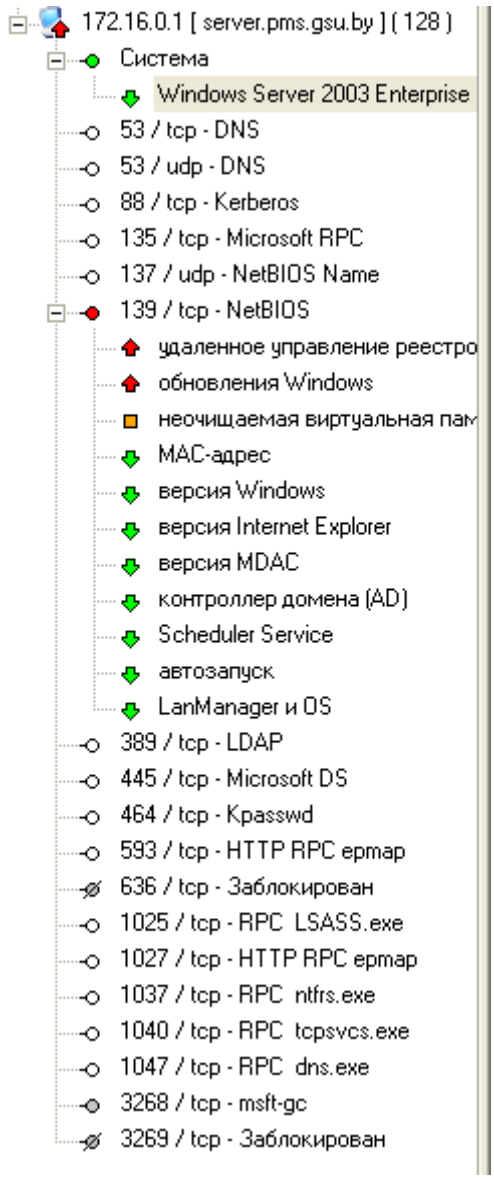
Шаг 1. На узле TWS2 перейдём в консоль XSpider. Создадим новый профиль сканирования.



Шаг 2. Включим опцию ICMP ping, отключим опцию TCP ping, отключим опцию «Сканировать не отвечающие хосты», в секции «Сканер портов» зададим параметр «Список портов» 1-200, в секции «Сканер уязвимостей» отключим опцию «Искать уязвимости».



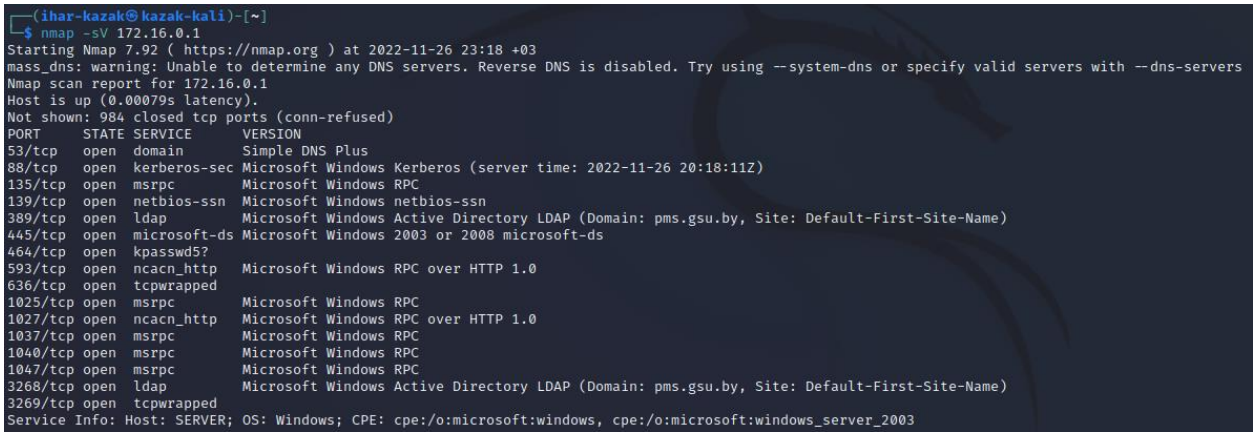
Шаг 3. Запустим сканирование служб и приложений сервера. Проверим, что службы FTP, SMTP, HTTP и другие найдены и идентифицированы.

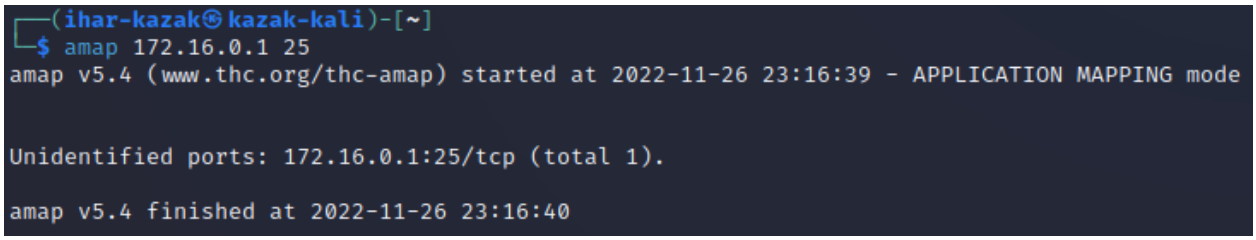


Шаг 4. Проверим наличие уязвимостей на сервере.

Уязвимость	Хост	Порт	Сервис
обновления Windows	172.16.0.1	139 / tcp	NetBIOS
удаленное управление реестром	172.16.0.1	139 / tcp	NetBIOS
неочищаемая виртуальная память	172.16.0.1	139 / tcp	NetBIOS
LanManager и OS	172.16.0.1	139 / tcp	NetBIOS
MAC-адрес	172.16.0.1	139 / tcp	NetBIOS
Scheduler Service	172.16.0.1	139 / tcp	NetBIOS
Windows Server 2003 Enterprise Edition (Service Pack 2)	172.16.0.1		
автозапуск	172.16.0.1	139 / tcp	NetBIOS
версия Internet Explorer	172.16.0.1	139 / tcp	NetBIOS
версия MDAC	172.16.0.1	139 / tcp	NetBIOS
версия Windows	172.16.0.1	139 / tcp	NetBIOS
контроллер домена (AD)	172.16.0.1	139 / tcp	NetBIOS

Шаг 5. На узле с помощью сетевых сканеров nmap и amap выполним идентификацию служб и приложений сервера: **nmap –sV 172.16.0.1, amap 172.16.0.1 25**





Вывод: в ходе лабораторной работы изучили и воспользовались методами и средствами идентификации служб и приложений, соответствующих открытым сетевым портам анализируемой КС.