Министерство образования Республики Беларусь
Учреждение образования
“Гомельский государственный университет им. Франциска Скорины”

# Отчёт по лабораторной работе №3

# «Идентификация служб и приложений»

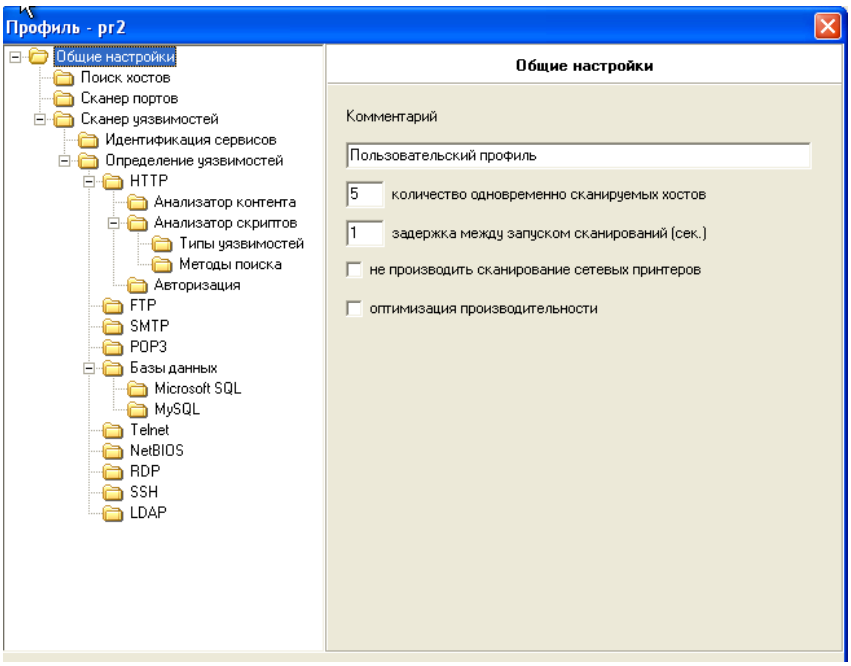
Выполнил:
Студент группы МС-42
Шалюта А.Н.
Проверил:
Старший преподаватель
Грищенко В.В.

2022

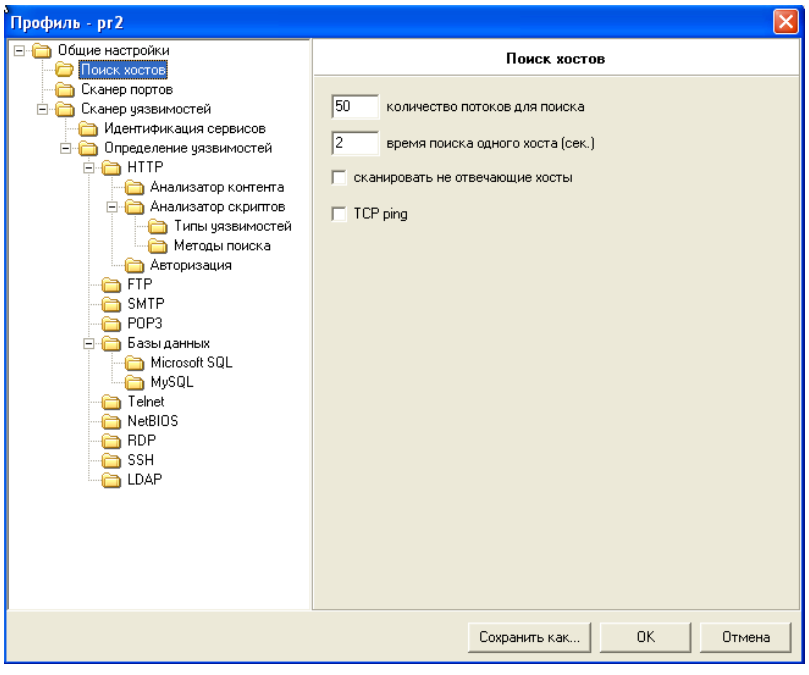
**Цель работы:** обучение методам и средствам идентификации служб иприложений, соответствующих открытым сетевым портам анализируемой КС.

## Ход работы.

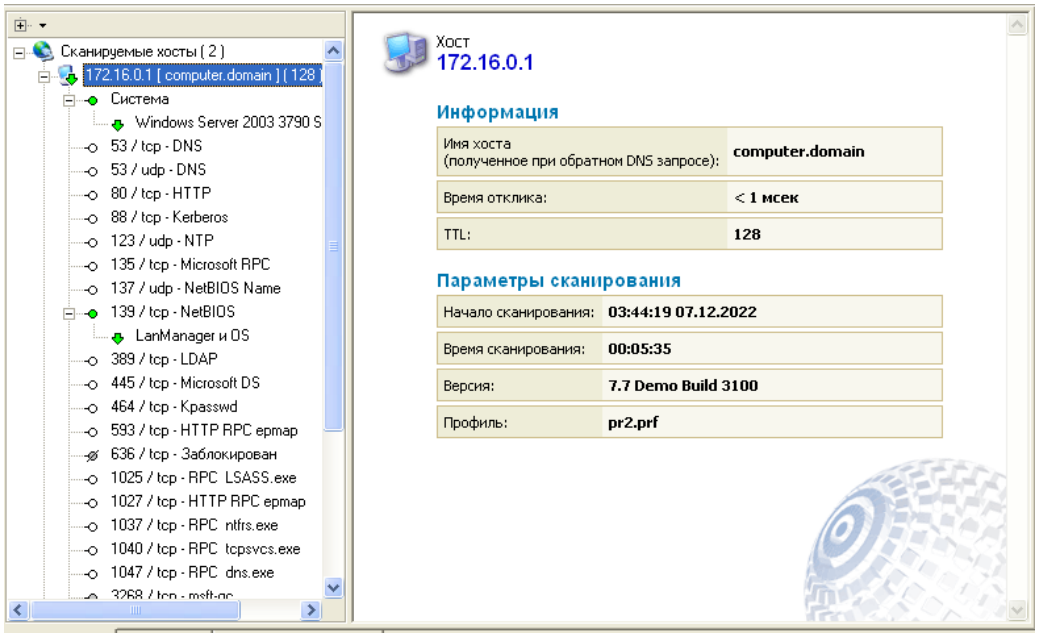
**Шаг 1.** На узле TWS2 перейдём в консоль XSpider. Создадим новый профильсканирования.

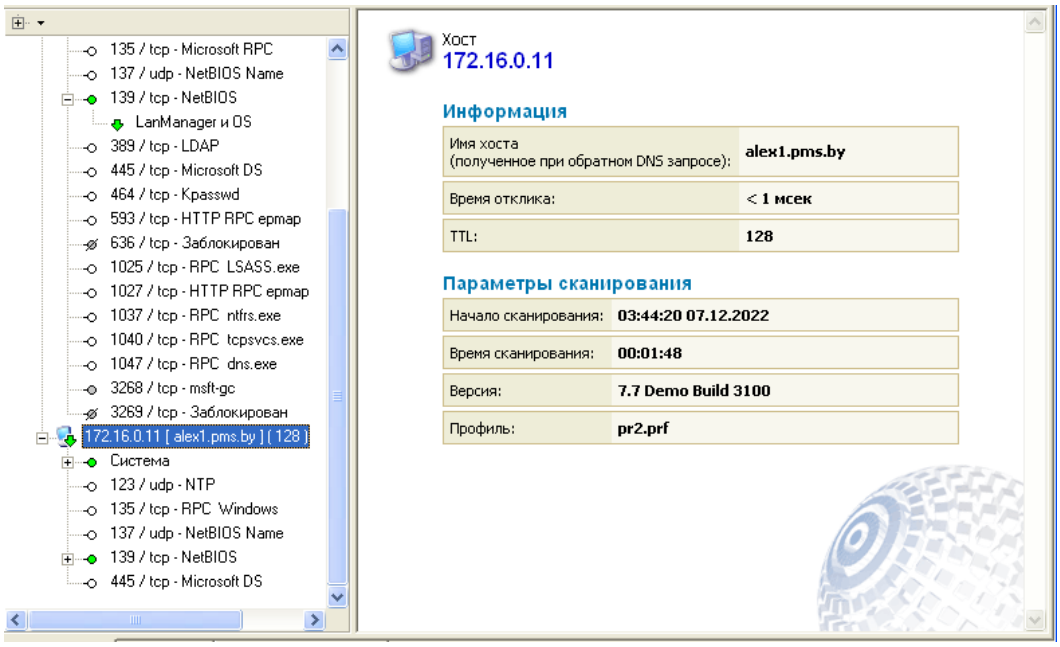



**Шаг 2.** Включим опцию ICMP ping, отключим опцию TCP ping, отключимопцию «Сканировать не отвечающие хосты», в секции «Сканер портов» зададим параметр «Список портов» 1-200, в секции «Сканер уязвимостей»отключим опцию «Искать уязвимости».



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



**Шаг 4.** Проверим наличие уязвимостей на сервере.

| Уязвимость | Хост | Порт | Сервис |
|---|---|---|---|
| LanManager и OS | 172.16.0.11 | 139 / tcp | |
| LanManager и OS | 172.16.0.1 | 139 / tcp | |
| Windows 5.1 | 172.16.0.11 | | |
| Windows Server 2003 3790 Service Pack 2 | 172.16.0.1 | | |

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

```
┌──(alex㉿kali)-[~]
└─$ nmap -sV 172.16.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-07 04:24 MSK
Nmap scan report for server.pms.by (172.16.0.1)
Host is up (0.00042s latency).
Not shown: 983 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
80/tcp   open  http         Microsoft IIS httpd 6.0
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2022
-12-07 01:24:19Z)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Doma
in: pms.by, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
1025/tcp open  msrpc        Microsoft Windows RPC
1027/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
1037/tcp open  msrpc        Microsoft Windows RPC
1040/tcp open  msrpc        Microsoft Windows RPC
1047/tcp open  msrpc        Microsoft Windows RPC
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Doma
in: pms.by, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: ALEXSERVER; OS: Windows; CPE: cpe:/o:microsoft:window
s, cpe:/o:microsoft:windows_server_2003

Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.00 seconds
```

**Вывод:** в ходе лабораторной работы изучили методы и средства идентификации служб и приложений, соответствующих открытым сетевым портам анализируемой КС.