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
Созинов Л.В.
Проверил:
Грищенко В.В.

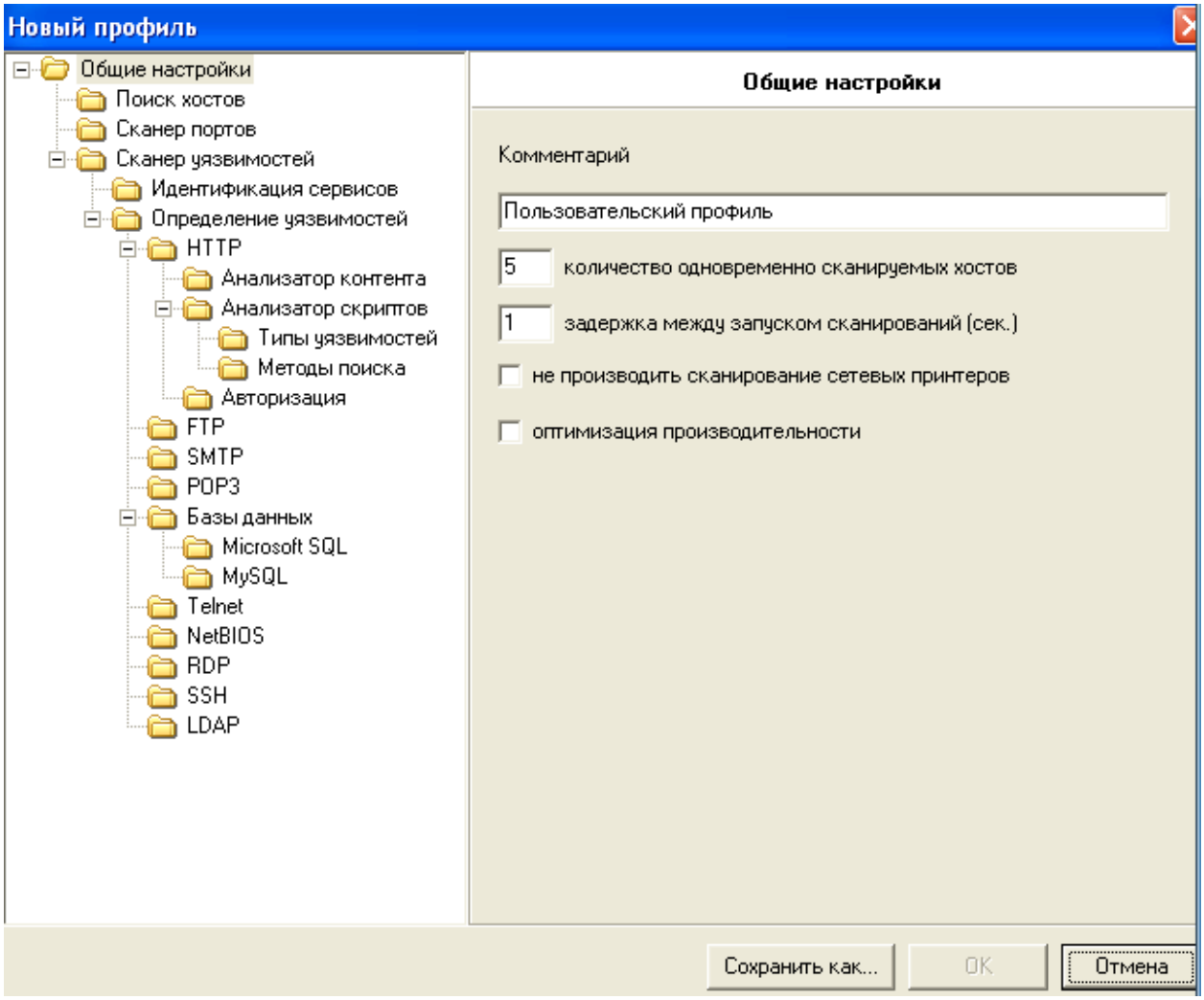
2022

Лабораторная работа №3
Идентификация служб и приложений

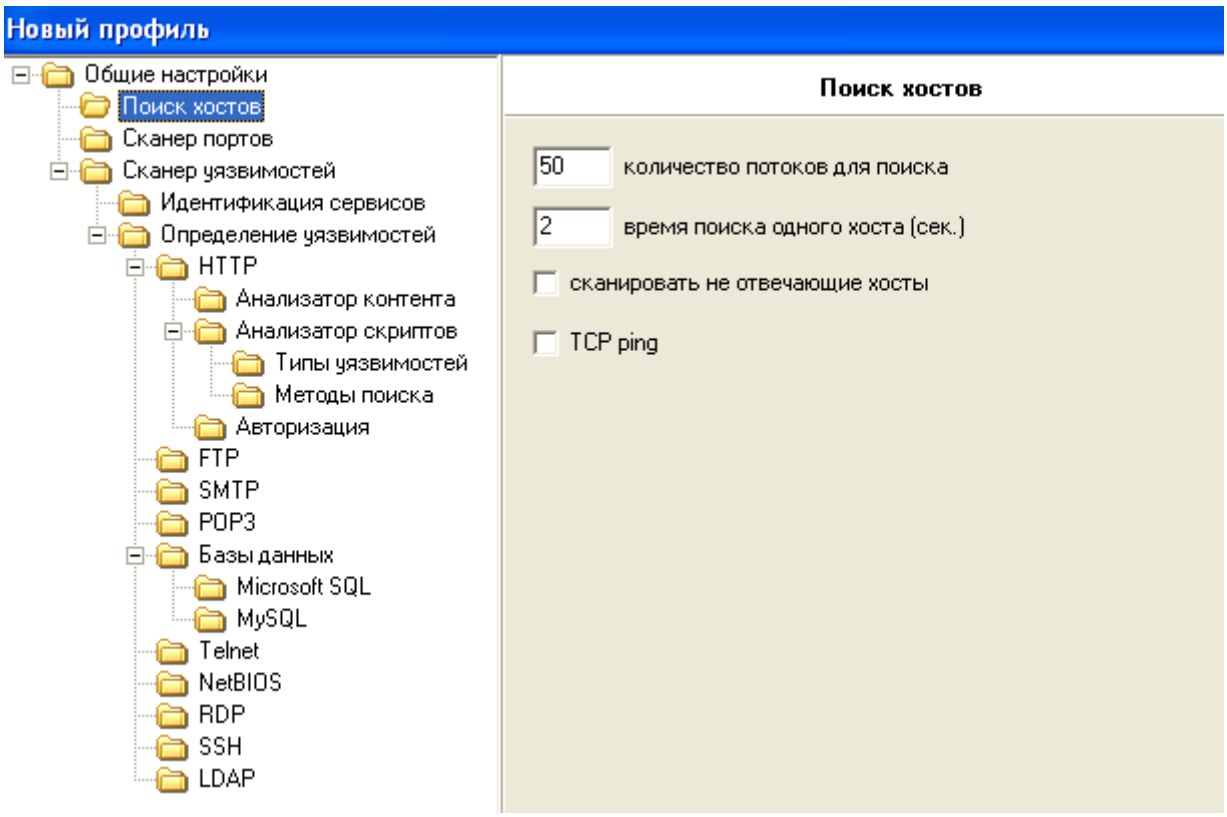
Цель работы: Обучение методам и средствам идентификации служб и приложений, соответствующих открытым сетевым портам анализируемой КС.

Ход работы

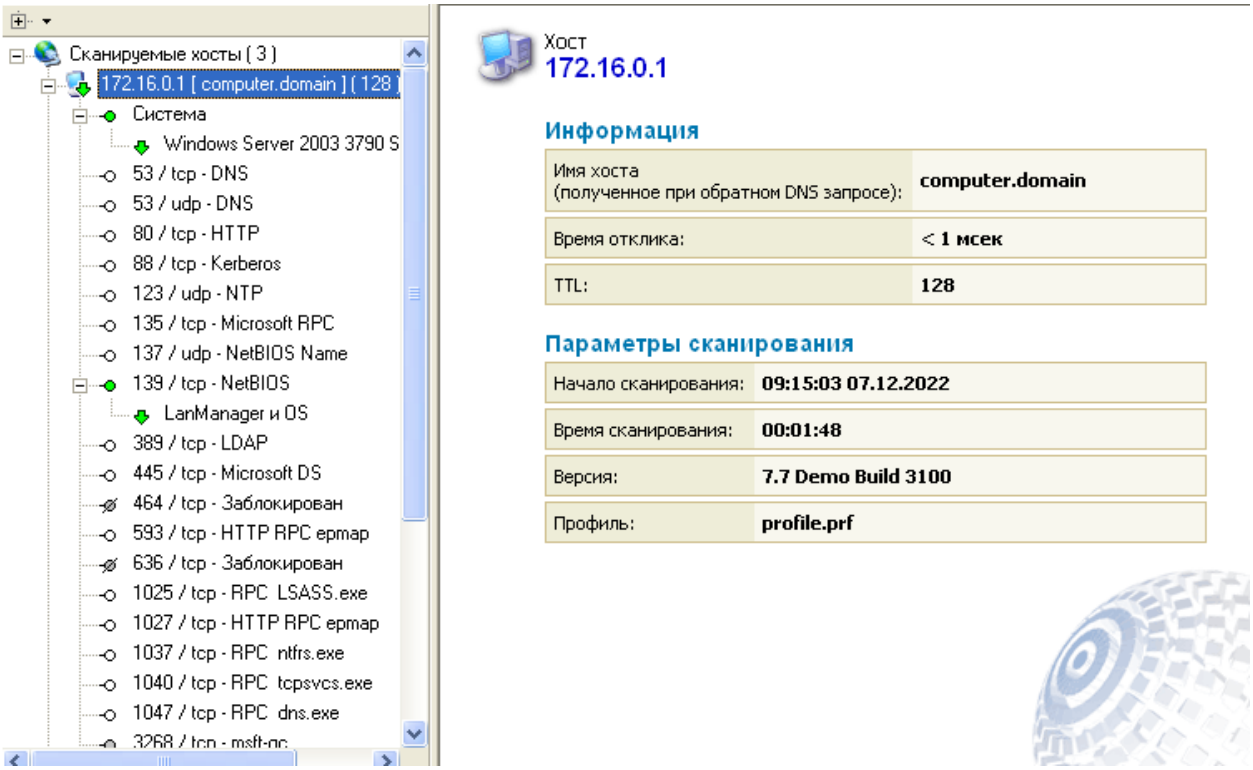
1. На узле TWS2 перейдём в консоль XSpider. Создадим новый профиль сканирования.

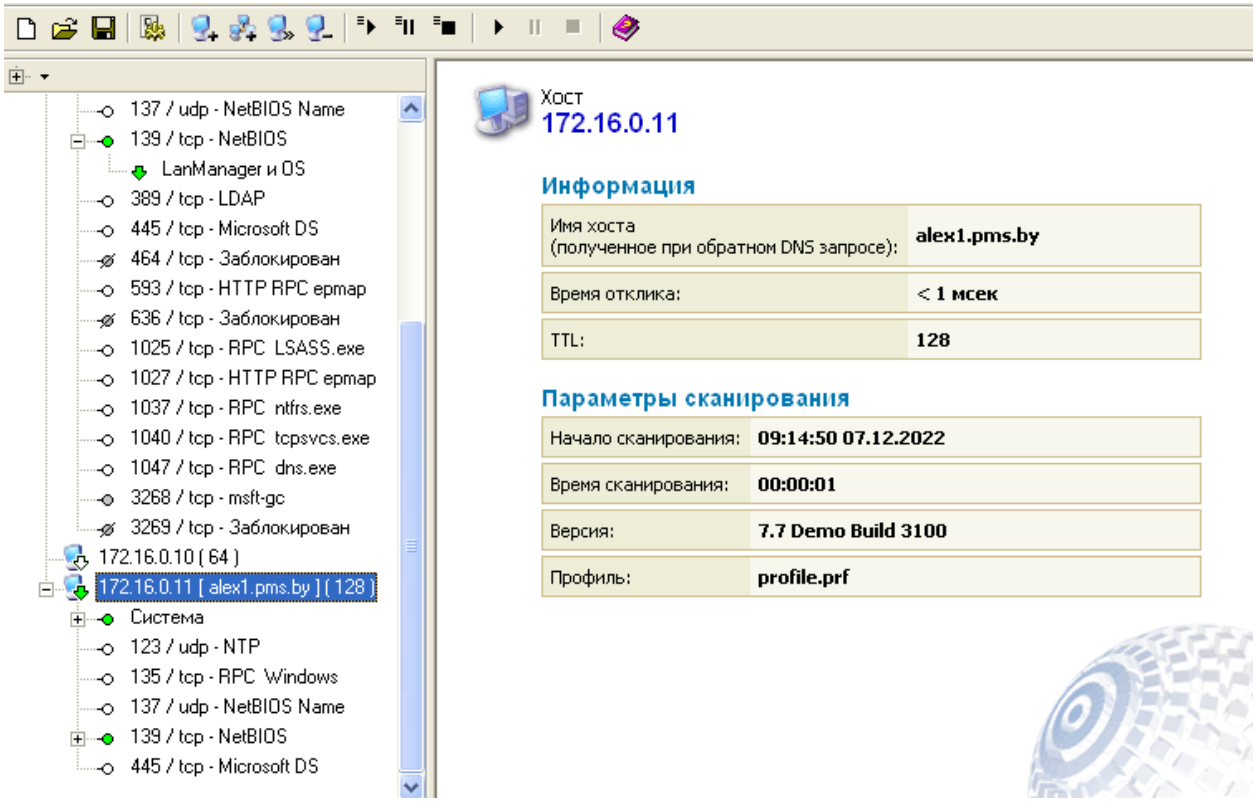


2. Включим опцию ICMP ping, отключим опцию TCP ping, отключим опцию «Сканировать не отвечающие хосты», в секции «Сканер портов» зададим параметр «Список портов» 1-200, в секции «Сканер уязвимостей» отключим опцию «Искать уязвимости».



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





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 Server 2003 3790 Service Pack 2	172.16.0.1		
Windows XP Professional [Service Pack 3]	172.16.0.11		

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

```
Nmap scan report for 172.16.0.1
Host is up (0.00068s 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 06:23:08Z)
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 (Domain:
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 (Domain:
pms.by, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: ALEXSERVER; OS: Windows; CPE: cpe:/o:microsoft:windows, c
pe:/o:microsoft:windows_server_2003

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.36 seconds
```