

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

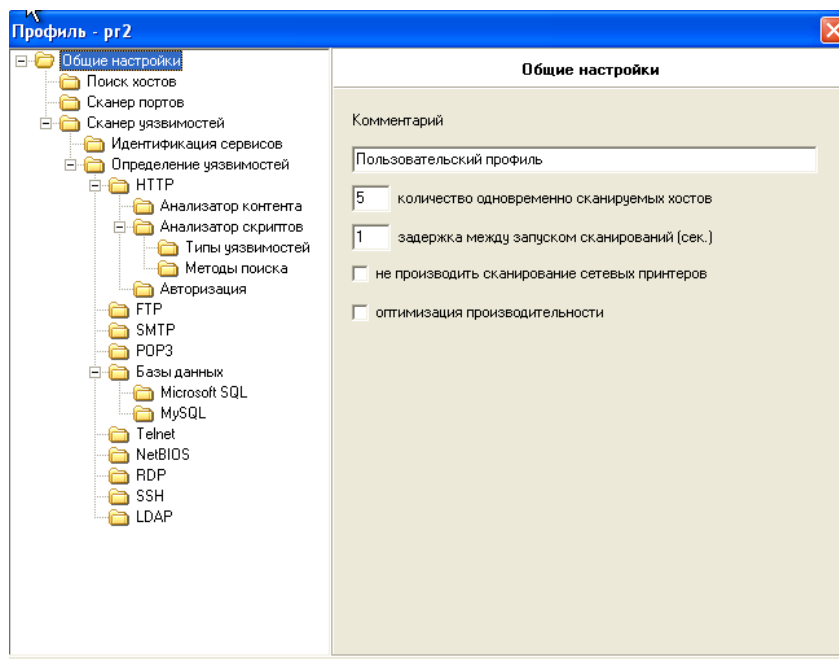
Отчёт по лабораторной работе №3
«Идентификация служб и приложений»

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

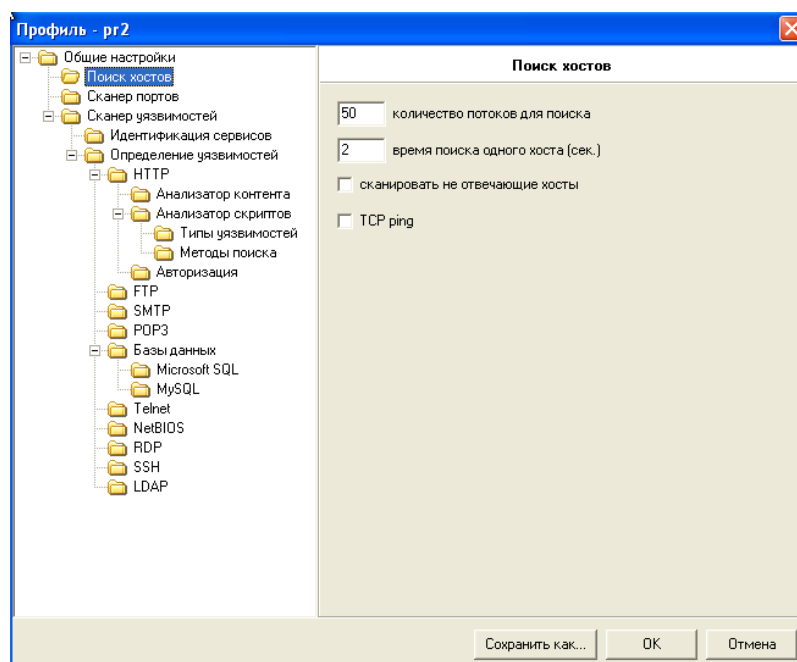
Цель работы: обучение методам и средствам идентификации служб и приложений, соответствующих открытым сетевым портам анализируемой КС.

Ход работы.

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



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.

The screenshot shows the Nmap ScanTool interface. On the left, a tree view under 'Сканируемые hosts (2)' shows the host '172.16.0.1 [computer.domain] ([128])' expanded. The 'Система' section lists various services: Windows Server 2003 3790 S, DNS (53/tcp, 53/udp), HTTP (80/tcp), Kerberos (88/tcp), NTP (123/udp), Microsoft RPC (135/tcp), NetBIOS Name (137/udp), NetBIOS (139/tcp), LanManager и OS, LDAP (389/tcp), Microsoft DS (445/tcp), Kpasswd (464/tcp), HTTP RPC ерmap (593/tcp), blocked (636/tcp), RPC LSASS.exe (1025/tcp), HTTP RPC ерmap (1027/tcp), RPC ntfrs.exe (1037/tcp), RPC tpsvcs.exe (1040/tcp), RPC dns.exe (1047/tcp), and msft-gc (3268/tcp). On the right, the 'Хост 172.16.0.1' section displays scan information and parameters.

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:	03:44:19 07.12.2022
Время сканирования:	00:05:35
Версия:	7.7 Demo Build 3100
Профиль:	pr2.prf

The screenshot shows the Nmap ScanTool interface. On the left, a tree view under 'Сканируемые hosts (2)' shows the host '172.16.0.11 [alex1.pms.by] ([128])' expanded. The 'Система' section lists various services: Microsoft RPC (135/tcp), NetBIOS Name (137/udp), NetBIOS (139/tcp), LanManager и OS, LDAP (389/tcp), Microsoft DS (445/tcp), Kpasswd (464/tcp), HTTP RPC ерmap (593/tcp), blocked (636/tcp), RPC LSASS.exe (1025/tcp), HTTP RPC ерmap (1027/tcp), RPC ntfrs.exe (1037/tcp), RPC tpsvcs.exe (1040/tcp), RPC dns.exe (1047/tcp), msft-gc (3268/tcp), blocked (3269/tcp), Windows (135/tcp), NetBIOS Name (137/udp), NetBIOS (139/tcp), and Microsoft DS (445/tcp). On the right, the 'Хост 172.16.0.11' section displays scan information and parameters.

Хост
172.16.0.11

Информация

Имя хоста (полученное при обратном DNS запросе):	alex1.pms.by
Время отклика:	< 1 мсек
TTL:	128

Параметры сканирования

Начало сканирования:	03:44:20 07.12.2022
Время сканирования:	00:01:48
Версия:	7.7 Demo Build 3100
Профиль:	pr2.prf

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 (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, 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.