

Министерство образования Республики Беларусь

Учреждение образования

“Гомельский государственный университет им. Франциска Скорины”

Отчёт по лабораторной работе №3

«Идентификация служб и приложений»

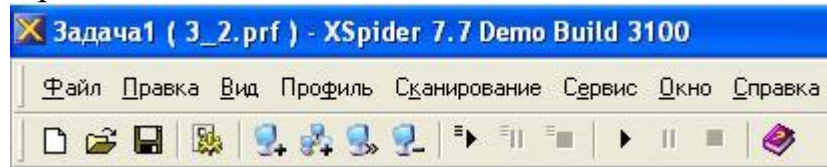
Выполнил:
Студент группы МС-42
Баль П.М.
Проверил: Грищенко В.В.

2022

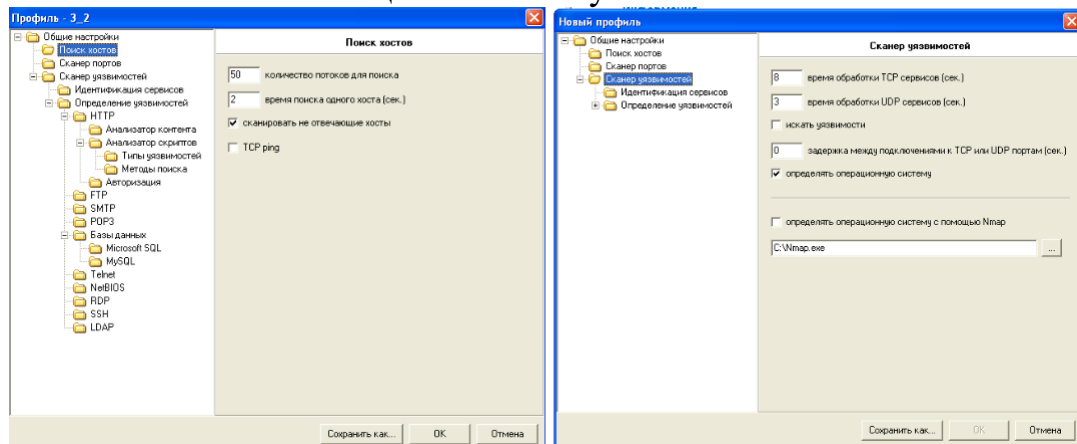
Лабораторная работа №3

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

Шаг 1. На узле TWS2 перейдем 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.

Сканируемые хосты (2)

- 172.16.0.1 [computer.domain] (128)
 - Система
 - Windows Server 2003 3790 Servi
 - 53 / tcp - DNS
 - 80 / tcp - HTTP
 - 88 / tcp - Kerberos
 - 135 / tcp - Microsoft RPC
 - 139 / tcp - NetBIOS
 - LanManager и OS
- 172.16.0.8 [alex1.pms.by] (128)
 - Система
 - Windows 5.1
 - 135 / tcp - RPC Windows
 - 139 / tcp - NetBIOS
 - LanManager и OS

Хост
172.16.0.1

Информация

Имя хоста (полученное при обратном DNS запросе):	computer.domain
Время отклика:	< 1 мсек
TTL:	128

Параметры сканирования

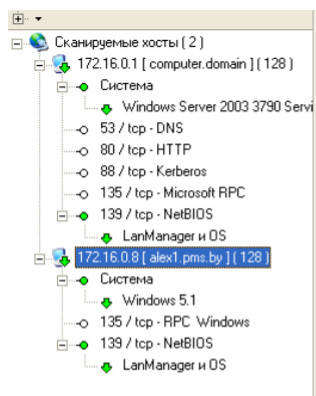
Начало сканирования:	13:05:54 20.11.2022
Время сканирования:	00:02:05
Версия:	7.7 Demo Build 3100
Профиль:	3_2.prf



Доступна информация
Windows Server 2003 3790 Service Pack 2

Описание

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



Хост
172.16.0.8

Информация

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

Параметры сканирования

Начало сканирования:	13:05:56 20.11.2022
Время сканирования:	00:01:21
Версия:	7.7 Demo Build 3100
Профиль:	3_2.prf



Доступна информация
Windows 5.1

Описание

Вероятная версия операционной системы : Windows 5.1

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 сканирования.

```

$ nmap -sV 172.16.0.8/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-03 15:51 MSK
Nmap scan report for server.pms.by (172.16.0.1)
Host is up (0.00032s 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: 2022-10-19 09:49:54Z)
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? Microsoft Windows RPC over HTTP 1.0
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

Nmap scan report for 172.16.0.9
Host is up (0.000055s latency).
All 1000 scanned ports on 172.16.0.9 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 57.91 seconds

$ amap 172.16.0.1 25
amap v5.4 (www.thc.org/thc-amap) started at 2022-12-03 15:50:05 - APPLICATION MAPPING mode
Unidentified ports: 172.16.0.1:25/tcp (total 1).
amap v5.4 finished at 2022-12-03 15:50:06
$ amap 172.16.0.1 21
amap v5.4 (www.thc.org/thc-amap) started at 2022-12-03 15:50:13 - APPLICATION MAPPING mode
Unidentified ports: 172.16.0.1:21/tcp (total 1).
amap v5.4 finished at 2022-12-03 15:50:13
```

Вывод: в ходе лабораторной работы были получены знания о методах и средствах идентификации служб и приложений, соответствующих открытым сетевым портам анализируемой КС.