

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

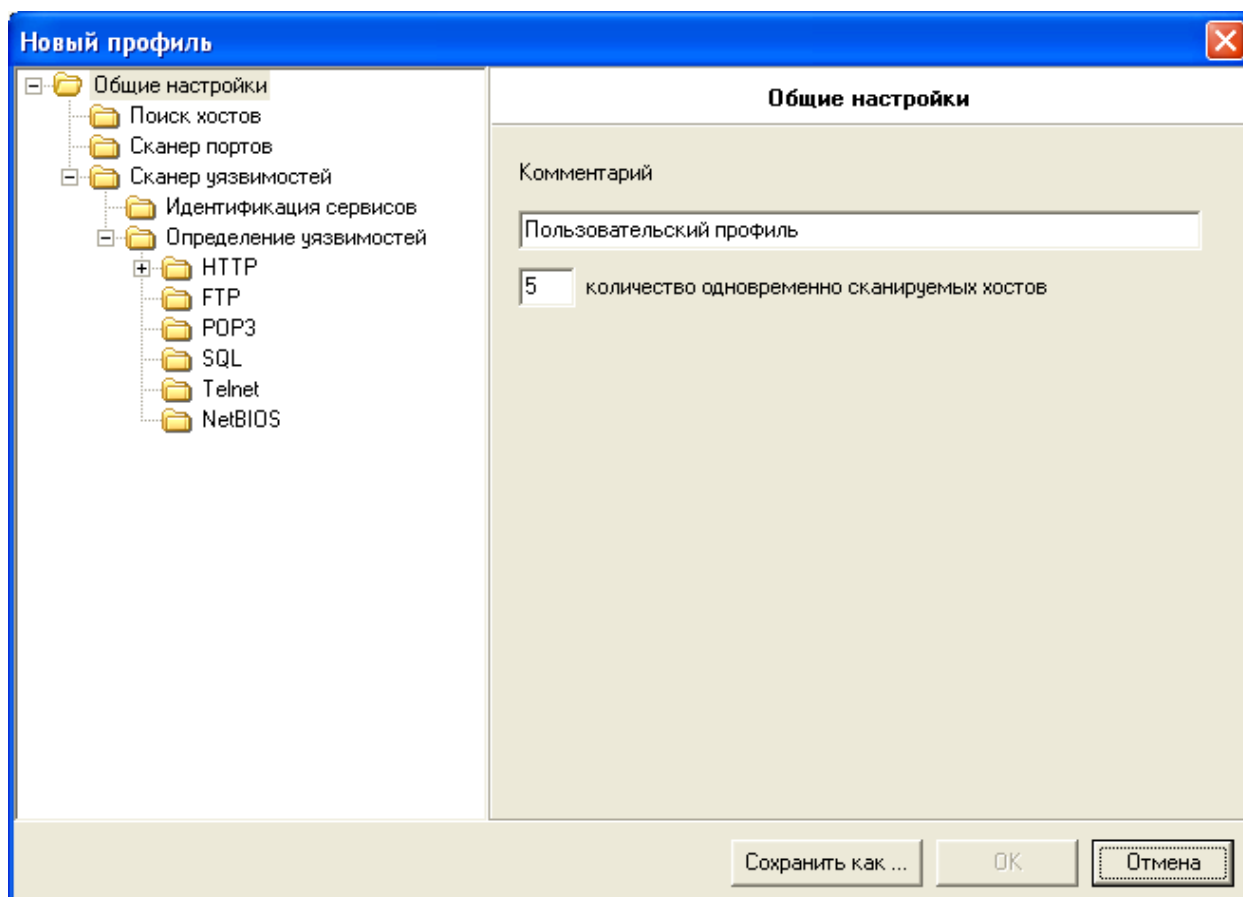
Грищенко В.В.

Гомель 2022

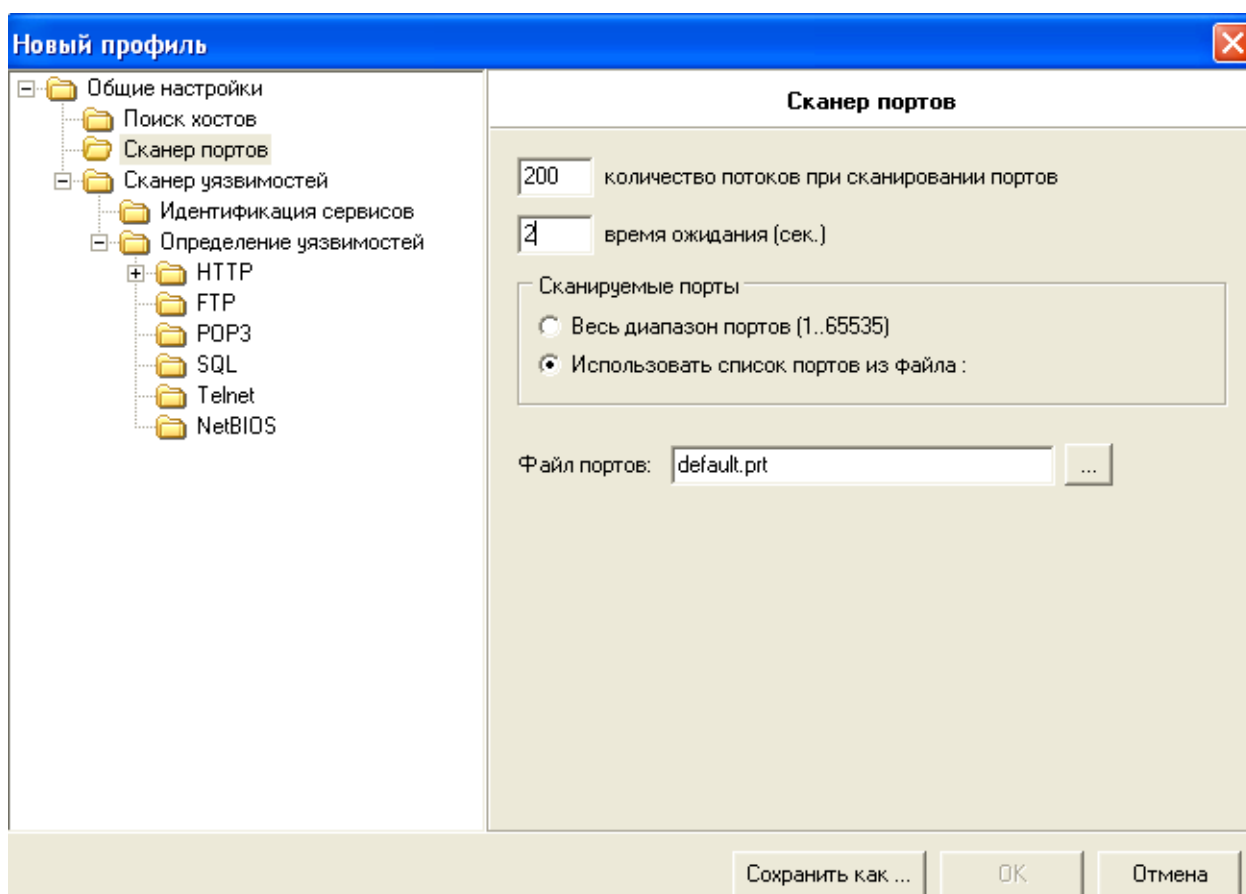
Цель работы: обучение методам и средствам идентификации служб и приложений, соответствующих открытым сетевым портам анализируемой КС.

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.

Хост
172.16.0.1

Информация

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

Параметры сканирования

Начало сканирования:	21:10:56 26.11.2022
Время сканирования:	00:03:41
Версия:	7.7 Build 3100
Профиль:	server.prf

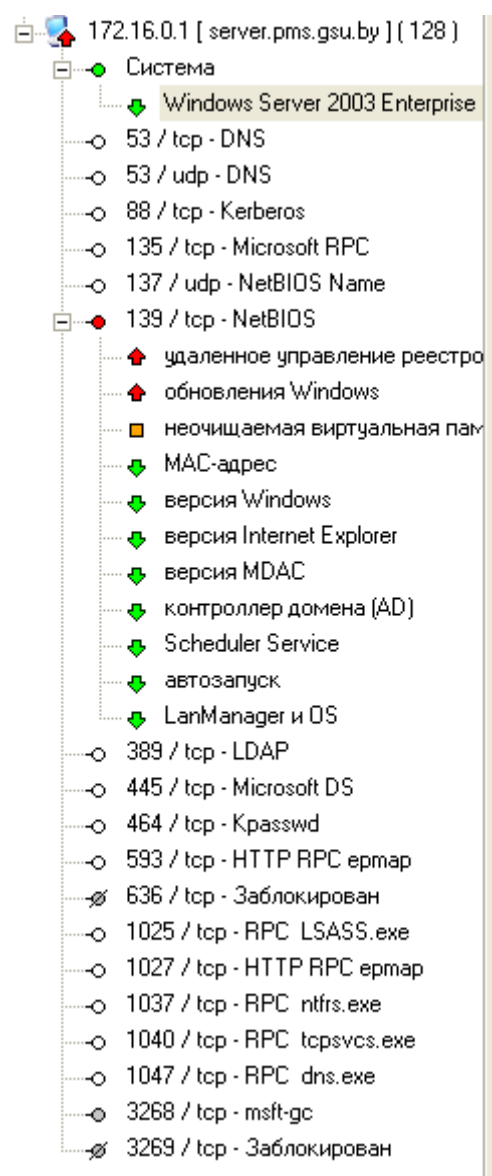


Доступна информация

Windows Server 2003 Enterprise Edition (Service Pack 2)

Описание

Вероятная версия операционной системы : Windows Server 2003 Enterprise Edition (Service Pack 2)



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**

```
(ihar-kazak@kazak-kali)-[~]
$ nmap -sV 172.16.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-26 23:18 +03
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.16.0.1
Host is up (0.00079s latency).
Not shown: 984 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Simple DNS Plus
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2022-11-26 20:18:11Z)
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.gsu.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.gsu.by, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
Service Info: Host: SERVER; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003
```

```
(ihar-kazak@kazak-kali)-[~]
$ amap 172.16.0.1 25
amap v5.4 (www.thc.org/thc-amap) started at 2022-11-26 23:16:39 - APPLICATION MAPPING mode

Unidentified ports: 172.16.0.1:25/tcp (total 1).

amap v5.4 finished at 2022-11-26 23:16:40
```

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