Министерство образования Республики Беларусь

Учреждение образования

“Гомельский государственный университет им. Франциска Скорины”

Отчёт по лабораторной работе №4

«Идентификация операционных систем»

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

2022

Лабораторная работа №4

Цель работы: обучение современным методам и средствам идентификации ОС анализируемой КС.

Постановка задачи: выполнить идентификацию ОС узлов сети и анализ возможностей сетевых сканеров.

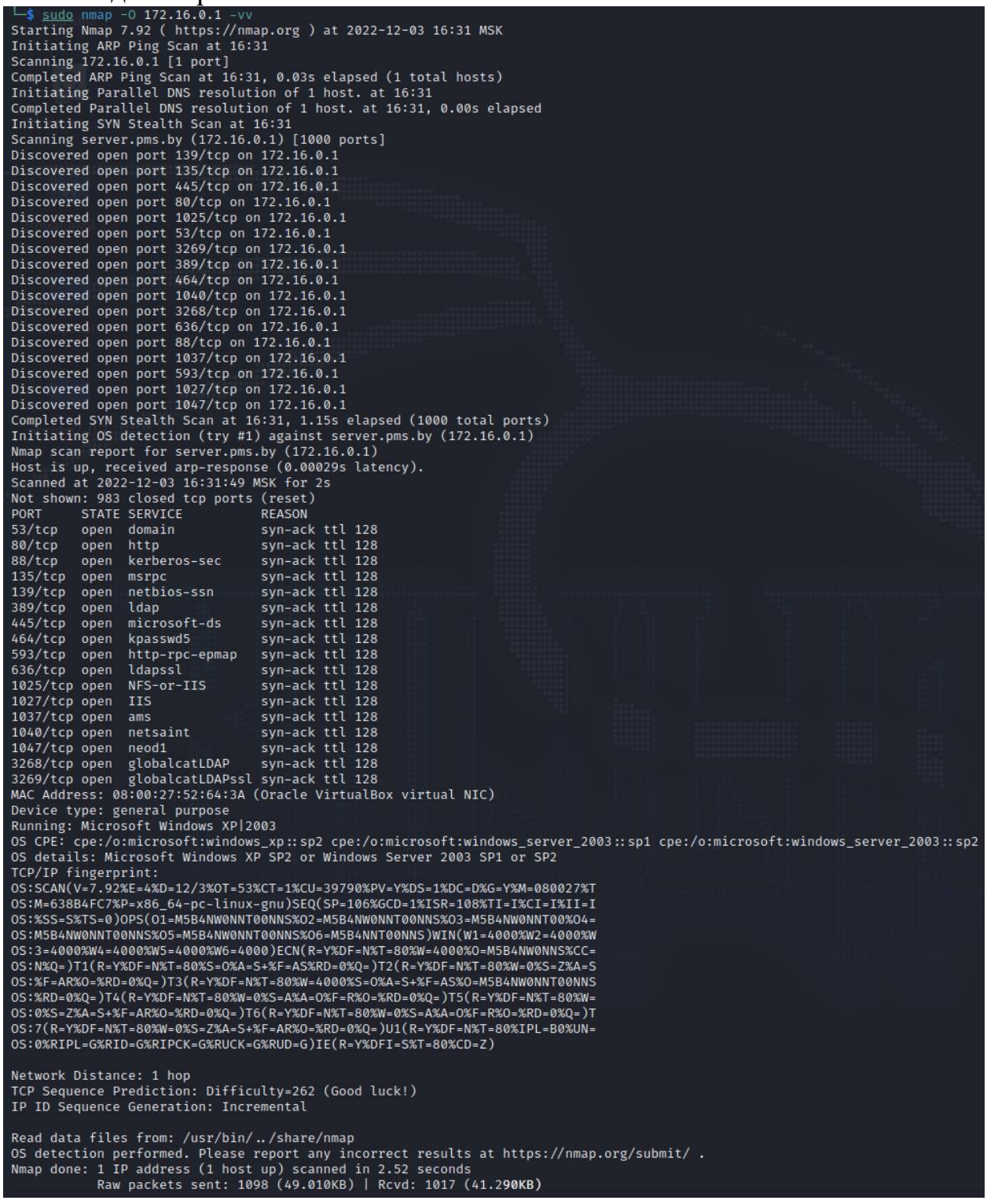
Шаг 1. Загрузить виртуальную машину TWS1. Войти в систему. Настроить сетевые интерфейсы. Запустить анализатор протоколов tcpdump или wireshark.

```
└─$ sudo tcpdump -D
1.eth0 [Up, Running, Connected]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]
```

Шаг 2. С помощью утилиты hping2 исследовать значения полей TTL в IP-заголовке и Window в TCP-заголовке для ОС семейства GNU/Linux и Windows соответственно:

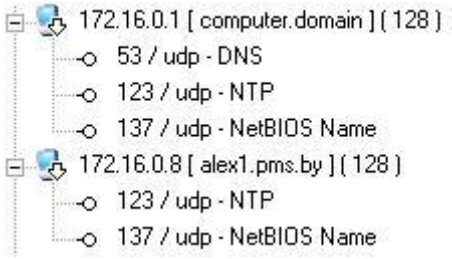
```
└─$ sudo hping3 -S -c 1 -p 25 172.16.0.9
HPING 172.16.0.9 (lo 172.16.0.9): S set, 40 headers + 0 data bytes
len=40 ip=172.16.0.9 ttl=64 DF id=0 sport=25 flags=RA seq=0 win=0 rtt=4.5 ms

── 172.16.0.9 hping statistic ──
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 4.5/4.5/4.5 ms
└─$ sudo hping3 -S -c 1 -p 80 172.16.0.9
HPING 172.16.0.9 (lo 172.16.0.9): S set, 40 headers + 0 data bytes
len=40 ip=172.16.0.9 ttl=64 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=4.5 ms

── 172.16.0.9 hping statistic ──
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 4.5/4.5/4.5 ms
```

Шаг 3. С помощью сетевого сканера nmap выполнить идентификацию ОС методом опроса стека TCP/IP:

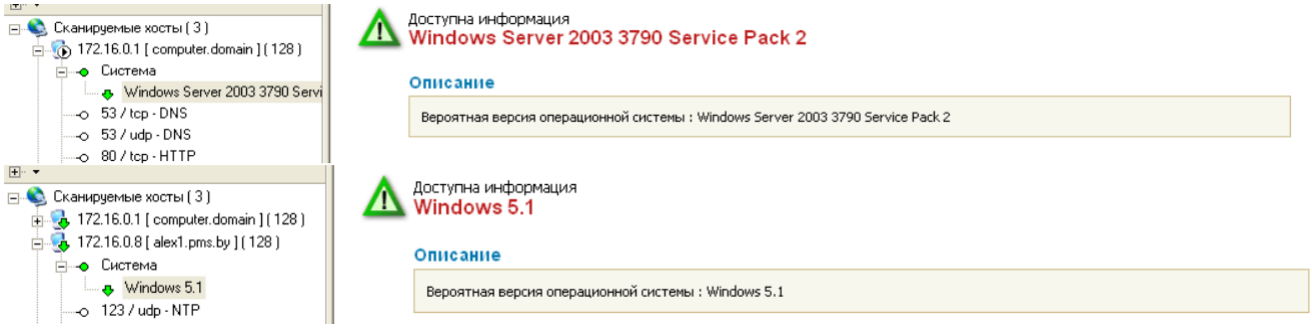


```
└─$ sudo nmap -O 172.16.0.1 -vv
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-03 16:31 MSK
Initiating ARP Ping Scan at 16:31
Scanning 172.16.0.1 [1 port]
Completed ARP Ping Scan at 16:31, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:31
Completed Parallel DNS resolution of 1 host. at 16:31, 0.00s elapsed
Initiating SYN Stealth Scan at 16:31
Scanning server.pms.by (172.16.0.1) [1000 ports]
Discovered open port 139/tcp on 172.16.0.1
Discovered open port 135/tcp on 172.16.0.1
Discovered open port 445/tcp on 172.16.0.1
Discovered open port 80/tcp on 172.16.0.1
Discovered open port 1025/tcp on 172.16.0.1
Discovered open port 53/tcp on 172.16.0.1
Discovered open port 3269/tcp on 172.16.0.1
Discovered open port 389/tcp on 172.16.0.1
Discovered open port 464/tcp on 172.16.0.1
Discovered open port 1040/tcp on 172.16.0.1
Discovered open port 3268/tcp on 172.16.0.1
Discovered open port 636/tcp on 172.16.0.1
Discovered open port 88/tcp on 172.16.0.1
Discovered open port 1037/tcp on 172.16.0.1
Discovered open port 593/tcp on 172.16.0.1
Discovered open port 1027/tcp on 172.16.0.1
Discovered open port 1047/tcp on 172.16.0.1
Completed SYN Stealth Scan at 16:31, 1.15s elapsed (1000 total ports)
Initiating OS detection (try #1) against server.pms.by (172.16.0.1)
Nmap scan report for server.pms.by (172.16.0.1)
Host is up, received arp-response (0.00029s latency).
Scanned at 2022-12-03 16:31:49 MSK for 2s
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE          REASON
53/tcp   open  domain           syn-ack ttl 128
80/tcp   open  http             syn-ack ttl 128
88/tcp   open  kerberos-sec     syn-ack ttl 128
135/tcp  open  msrpc            syn-ack ttl 128
139/tcp  open  netbios-ssn      syn-ack ttl 128
389/tcp  open  ldap             syn-ack ttl 128
445/tcp  open  microsoft-ds     syn-ack ttl 128
464/tcp  open  kpasswd5         syn-ack ttl 128
593/tcp  open  http-rpc-epmap   syn-ack ttl 128
636/tcp  open  ldapssl          syn-ack ttl 128
1025/tcp open  NFS-or-IIS       syn-ack ttl 128
1027/tcp open  IIS              syn-ack ttl 128
1037/tcp open  ams              syn-ack ttl 128
1040/tcp open  netsaint         syn-ack ttl 128
1047/tcp open  neod1            syn-ack ttl 128
3268/tcp open  globalcatLDAP    syn-ack ttl 128
3269/tcp open  globalcatLDAPssl syn-ack ttl 128
MAC Address: 08:00:27:52:64:3A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=12/3%OT=53%CT=1%CU=39790%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=638B4FC7%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=108%TI=I%CI=I%II=I
OS:%SS=S%TS=0)OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=
OS:M5B4NW0NNT00NNS%O5=M5B4NW0NNT00NNS%O6=M5B4NNT00NNS)WIN(W1=4000%W2=4000%W
OS:3=4000%W4=4000%W5=4000%W6=4000)ECN(R=Y%DF=N%T=80%W=4000%O=M5B4NW0NNS%CC=
OS:N%Q=)T1(R=Y%DF=N%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=N%T=80%W=0%S=Z%A=S
OS:%F=AR%O=%RD=0%Q=)T3(R=Y%DF=N%T=80%W=4000%S=O%A=S+%F=AS%O=M5B4NW0NNT00NNS
OS:%RD=0%Q=)T4(R=Y%DF=N%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=80%W=
OS:0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=N%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T
OS:7(R=Y%DF=N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=B0%UN=
OS:0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=80%CD=Z)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.52 seconds
           Raw packets sent: 1098 (49.010KB) | Rcvd: 1017 (41.290KB)
```

Шаг 4. На узле TWS2 перейти в консоль XSpider. Обратить внимание на результаты определения ОС в ходе предыдущих сканирований. В используемом профиле сократить диапазон портов до 1–30 и выполнить повторное сканирование. Убедиться, что ОС не определена.



Шаг 5. В профили сканирования включить опции «Искать уязвимости», «Искать скрытые каталоги». Выполнить сканирование. убедиться в том, что ОС идентифицирована.



Вывод: в ходе лабораторной работы были изучены современные методы и средства идентификации ОС анализируемой КС, выполнена идентификация ОС узлов сети и анализ возможностей сетевых сканеров.