Министерство образования Республики Беларусь
Учреждение образования
«Гомельский государственный университет
имени Франциска Скорины»

Отчёт по лабораторной работе №4
«Идентификация операционных систем»

Выполнил студент группы МС-42: Казак И.В.
Проверил:
Старший преподаватель Грищенко В.В.

Гомель 2022

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

Ход работы.

Шаг 1. Загрузим виртуальную машину. Войдём в систему. Настроим сетевые интерфейсы. Запустим анализатор протоколов **tcpdump**.

```
┌──(ihar-kazak㉿kazak-kali)-[~]
└─$ sudo tcpdump -D
[sudo] password for ihar-kazak:
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 исследуем значения полей TTL в IP-заголовке и Window в TCP-заголовке для ОС семейства GNU/Linux и Windows соответственно: (Windows – 128, Linux - 64).

```
┌──(ihar-kazak㉿kazak-kali)-[~]
└─$ sudo hping3 -S -c 1 -p 80 172.16.0.20
HPING 172.16.0.20 (eth0 172.16.0.20): S set, 40 headers + 0 data bytes
len=46 ip=172.16.0.20 ttl=128 id=11547 sport=80 flags=RA seq=0 win=0 rtt=2.7 ms

--- 172.16.0.20 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2.7/2.7/2.7 ms

┌──(ihar-kazak㉿kazak-kali)-[~]
└─$
```

```
┌──(ihar-kazak㉿kazak-kali)-[~]
└─$ sudo hping3 -S -c 1 -p 25 172.16.0.20
HPING 172.16.0.20 (eth0 172.16.0.20): S set, 40 headers + 0 data bytes
len=46 ip=172.16.0.20 ttl=128 id=11548 sport=25 flags=RA seq=0 win=0 rtt=3.7 ms

--- 172.16.0.20 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.7/3.7/3.7 ms
```

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

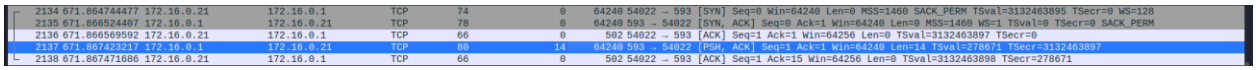
nmap –O 172.16.0.1 –vv

```
Nmap scan report for 172.16.0.1
Host is up, received arp-response (0.00065s latency).
Scanned at 2022-11-26 23:30:11 +03 for 4s
Not shown: 984 closed tcp ports (reset)
PORT     STATE SERVICE          REASON
53/tcp   open  domain           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: 08:00:27:01:C9:43 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 2003
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows Server 2003 SP1 or SP2
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=11/26%OT=53%CT=1%CU=41035%PV=Y%DS=1%DC=D%G=N%M=080027%
OS:TM=63827758%P=x86_64-pc-linux-gnu)SEQ(SP=FA%GCD=1%ISR=FC%TI=I%CI=I%II=I%
OS:SS=S%TS=0)OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M
OS:5B4NW0NNT00NNS%O5=M5B4NW0NNT00NNS%O6=M5B4NNT00NNS)WIN(W1=FAF0%W2=FAF0%W3
OS:=FAF0%W4=FAF0%W5=FAF0%W6=FAF0)ECN(R=Y%DF=N%T=80%W=FAF0%O=M5B4NW0NNS%CC=N
OS:%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=FAF0%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=0
OS:%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=)T7
OS:(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=0
OS:%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=251 (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 5.85 seconds
           Raw packets sent: 1114 (50.428KB) | Rcvd: 1033 (42.480KB)
```

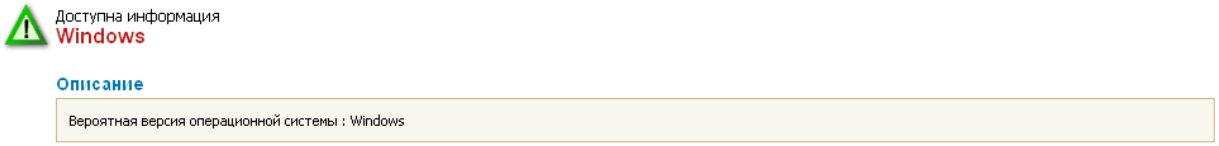
Шаг 4. С помощью утилиты Wireshark определить тип ОС сервера.



TTL=128 => Windows, TCP Window Size = 64240 => Windows Server 2003

Шаг 5. 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.

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



Вывод: в ходе лабораторной работы познакомились и воспользовались современными методами и средствами идентификации ОС анализируемой КС.