

УО «Гомельский государственный университет им. Ф. Скорины»
Физический факультет
Кафедра общей физики

ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 4

Идентификация операционных систем

Проверил:
Грищенко В.В.

Выполнили:
студент группы МС-42
Гончаров Владислав

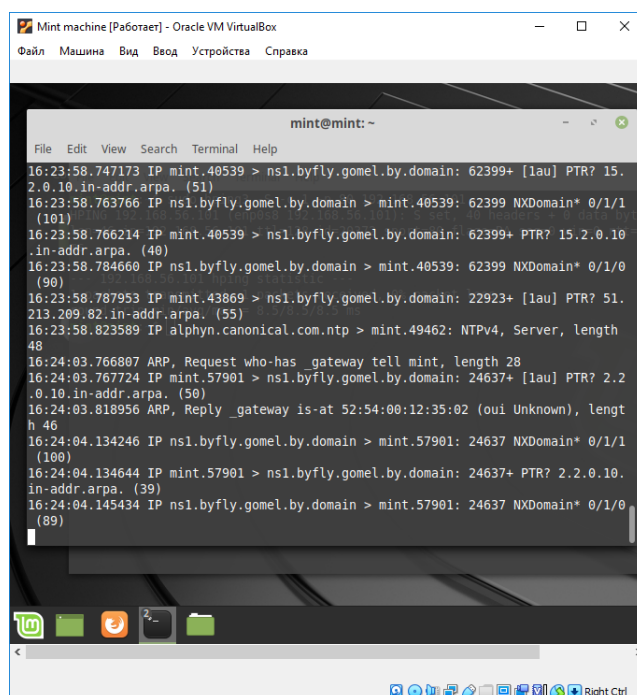
Гомель 2020

Лабораторная работа №4

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

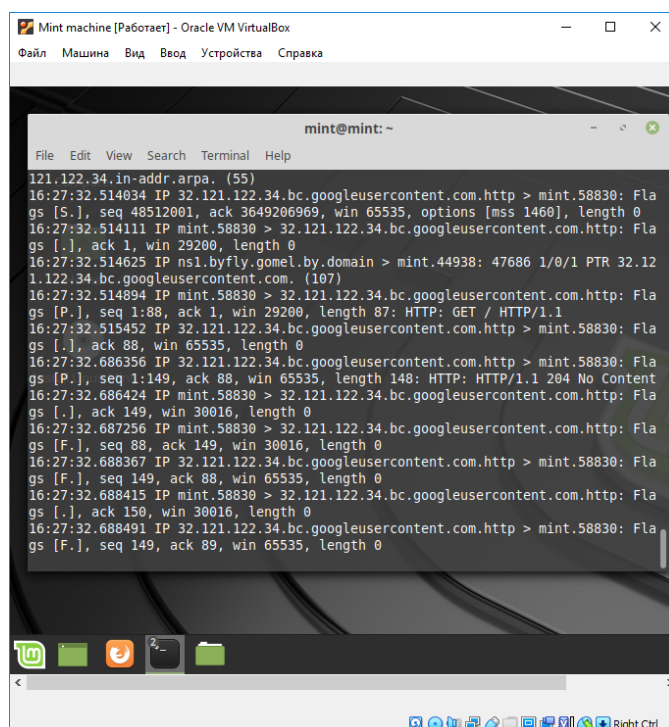
Постановка задачи: выполнить идентификацию ОС узлов сети и анализ возможностей сетевых сканеров.

Шаг 1. Запустить анализатор протоколов tcpdump или wireshark. Ниже приведены скриншоты утилиты tcpdump в процесс всей выполнения работы.



```
Mint machine [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

mint@mint: ~
File Edit View Search Terminal Help
16:23:58.747173 IP mint.40539 > ns1.byfly.gomel.by.domain: 62399+ [Iau] PTR? 15.
2.0.10.in-addr.arpa. (51)
16:23:58.763766 IP ns1.byfly.gomel.by.domain > mint.40539: 62399 NXDomain* 0/1/1
(101)
16:23:58.766214 IP mint.40539 > ns1.byfly.gomel.by.domain: 62399+ PTR? 15.2.0.10
.in-addr.arpa. (40)
16:23:58.784660 IP ns1.byfly.gomel.by.domain > mint.40539: 62399 NXDomain* 0/1/0
(90)
16:23:58.787953 IP mint.43869 > ns1.byfly.gomel.by.domain: 22923+ [Iau] PTR? 51.
213.209.82.in-addr.arpa. (55)
16:23:58.823589 IP alphyn.canonical.com.ntp > mint.49462: NTPv4, Server, length
48
16:24:03.766807 ARP, Request who-has _gateway tell mint, length 28
16:24:03.767724 IP mint.57901 > ns1.byfly.gomel.by.domain: 24637+ [Iau] PTR? 2.2
.0.10.in-addr.arpa. (50)
16:24:03.818956 ARP, Reply _gateway is-at 52:54:00:12:35:02 (oui Unknown), lengt
h 46
16:24:04.134246 IP ns1.byfly.gomel.by.domain > mint.57901: 24637 NXDomain* 0/1/1
(100)
16:24:04.134644 IP mint.57901 > ns1.byfly.gomel.by.domain: 24637+ PTR? 2.2.0.10.
in-addr.arpa. (39)
16:24:04.145434 IP ns1.byfly.gomel.by.domain > mint.57901: 24637 NXDomain* 0/1/0
(89)
```



```
Mint machine [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

mint@mint: ~
File Edit View Search Terminal Help
121.122.34.in-addr.arpa. (55)
16:27:32.514034 IP 32.121.122.34.bc.googleusercontent.com.http > mint.58830: Fla
gs [S.], seq 48512001, ack 3649206969, win 65535, options [mss 1460], length 0
16:27:32.514111 IP mint.58830 > 32.121.122.34.bc.googleusercontent.com.http: Fla
gs [.] , ack 1, win 29200, length 0
16:27:32.514625 IP ns1.byfly.gomel.by.domain > mint.44938: 47686 1/0/1 PTR 32.12
1.122.34.bc.googleusercontent.com. (107)
16:27:32.514894 IP mint.58830 > 32.121.122.34.bc.googleusercontent.com.http: Fla
gs [P.], seq 1:88, ack 1, win 29200, length 87: HTTP: GET / HTTP/1.1
16:27:32.515452 IP 32.121.122.34.bc.googleusercontent.com.http > mint.58830: Fla
gs [.] , ack 88, win 65535, length 0
16:27:32.686356 IP 32.121.122.34.bc.googleusercontent.com.http > mint.58830: Fla
gs [P.], seq 1:149, ack 88, win 65535, length 148: HTTP: HTTP/1.1 204 No Content
16:27:32.686424 IP mint.58830 > 32.121.122.34.bc.googleusercontent.com.http: Fla
gs [.] , ack 149, win 30016, length 0
16:27:32.687256 IP mint.58830 > 32.121.122.34.bc.googleusercontent.com.http: Fla
gs [F.], seq 88, ack 149, win 30016, length 0
16:27:32.688367 IP 32.121.122.34.bc.googleusercontent.com.http > mint.58830: Fla
gs [F.], seq 149, ack 88, win 65535, length 0
16:27:32.688415 IP mint.58830 > 32.121.122.34.bc.googleusercontent.com.http: Fla
gs [.] , ack 150, win 30016, length 0
16:27:32.688491 IP 32.121.122.34.bc.googleusercontent.com.http > mint.58830: Fla
gs [F.], seq 149, ack 89, win 65535, length 0
```


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

```
Mint machine [Работаю] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

mint@mint: ~
File Edit View Search Terminal Help

mint@mint:~$ sudo nmap -O 192.168.56.101 -vv
Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-23 16:27 UTC
Initiating ARP Ping Scan at 16:27
Scanning 192.168.56.101 [1 port]
Completed ARP Ping Scan at 16:27; 0.24s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:27
Completed Parallel DNS resolution of 1 host. at 16:27; 0.00s elapsed
Initiating SYN Stealth Scan at 16:27
Scanning 192.168.56.101 [1000 ports]
Discovered open port 445/tcp on 192.168.56.101
Discovered open port 139/tcp on 192.168.56.101
Discovered open port 135/tcp on 192.168.56.101
Increasing send delay for 192.168.56.101 from 0 to 5 due to 194 out of 646 dropped probes since last increase.
Increasing send delay for 192.168.56.101 from 5 to 10 due to 22 out of 72 dropped probes since last increase.
Completed SYN Stealth Scan at 16:27; 3.73s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.56.101
Nmap scan report for 192.168.56.101
Host is up, received arp-response (0.00080s latency).
Scanned at 2020-12-23 16:27:03 UTC for 7s
Not shown: 997 closed ports
Reason: 997 resets
```

```
Mint machine [Работаю] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

mint@mint: ~
File Edit View Search Terminal Help

PORT      STATE SERVICE 121.122.34.bc.googleusercontent.com http > mint.58830: Fla
135/tcp open  msrpc    syn-ack ttl 128 65535, options [mss 1460], length 0
139/tcp open  netbios-ssn syn-ack ttl 128 34.bc.googleusercontent.com http: Fla
445/tcp open  microsoft-ds syn-ack ttl 128
MAC Address: 08:00:27:31:5B:85 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=12/23%OT=135%CT=1%CU=43871%PV=Y%DS=1%DC=D%G=Y%M=080027
OS:%TM=5FE36FDE%P=i686-pc-linux-gnu)SEQ(SP=F5%GCD=1%ISR=106%TI=I%CI=I%TS=0)
OS:OPS(O1=M5B4NW0NNT00NNS%02=M5B4NW0NNT00NNS%03=M5B4NW0NNT00%04=M5B4NW0NNT0
OS:0NNS%05=M5B4NW0NNT00NNS%06=M5B4NNT00NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=F
OS:FFF%W5=FFF%W6=FFF)ECN(R=Y%DF=Y%T=80%W=FFF%O=M5B4NW0NNS%CC=N%Q=)T1(R=Y
OS:%DF=Y%T=80%S=0%A=S+F=AS%RD=0%Q=)T2(R=Y%DF=N%T=80%W=0%S=Z%A=S%F=AR%0=RD
OS:=0%Q=)T3(R=Y%DF=Y%T=80%W=FFF%S=0%A=S+F=AS%O=M5B4NW0NNT00NNS%RD=0%Q=)T4
OS:(R=Y%DF=N%T=80%W=0%S=A%A=0%F=R%O=RD=0%Q=)T5(R=Y%DF=N%T=80%W=0%S=Z%A=S+
OS:F=AR%0=RD=0%Q=)T6(R=Y%DF=N%T=80%W=0%S=A%A=0%F=R%O=RD=0%Q=)T7(R=Y%DF=N%
OS:T=80%W=0%S=Z%A=S+F=AR%0=RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=B0%UN=0%RIPL=G%RI
OS:D=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=80%CD=Z)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=245 (Good luck!)
```

```
Mint machine [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

mint@mint: ~

File Edit View Search Terminal Help

139/tcp open  netbios-ssn syn-ack ttl 128
445/tcp open  microsoft-ds syn-ack ttl 128
MAC Address: 08:00:27:31:5B:85 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=12/23%OT=135%CT=1%CU=43871%PV=Y%DS=1%DC=D%G=Y%M=080027
OS:TM=5FE36FDE%P=i686-pc-linux-gnu)SEQ(SP=F5%GCD=1%ISR=106%TI=I%CI=I%TS=0)
OS:OPS(O1=M5B4NW0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M5B4NW0NNT0
OS:0NNS%O5=M5B4NW0NNT00NNS%O6=M5B4NNT00NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=F
OS:FFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW0NNS%CC=N%Q=)T1(R=Y
OS:%DF=Y%T=80%W=0%A=S+F=AS%RD=0%Q=)T2(R=Y%DF=N%T=80%W=0%S=Z%A=S+F=AR%O=RD
OS:=0%Q=)T3(R=Y%DF=Y%T=80%W=FFFF%S=0%A=S+F=AS%O=M5B4NW0NNT00NNS%RD=0%Q=)T4
OS:(R=Y%DF=N%T=80%W=0%S=A%A=0F=R%O=RD=0%Q=)T5(R=Y%DF=N%T=80%W=0%S=Z%A=S+
OS:F=AR%O=RD=0%Q=)T6(R=Y%DF=N%T=80%W=0%S=A%A=0F=R%O=RD=0%Q=)T7(R=Y%DF=N%
OS:T=80%W=0%S=Z%A=S+F=AR%O=RD=0%Q=)UI1(R=Y%DF=N%T=80%IPL=80%UN=0%RIPL=G%RI
OS:D=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=80%CD=Z)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=245 (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/submi
Nmap done: 1 IP address (1 host up) scanned in 7.93 seconds
Raw packets sent: 1293 (59.452KB) | Rcvd: 1292 (53.488KB)

mint@mint: ~
Firefox Web Browser
```

Шаг 4. С помощью сетевого сканера xprobe выполнить идентификацию ОС с использованием опроса модуля ICMP. Проанализировать результаты сканирования, сравнить с результатами использования сканера Nmap. Проанализировать трассировки.

```
Mint machine [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

mint@mint: ~

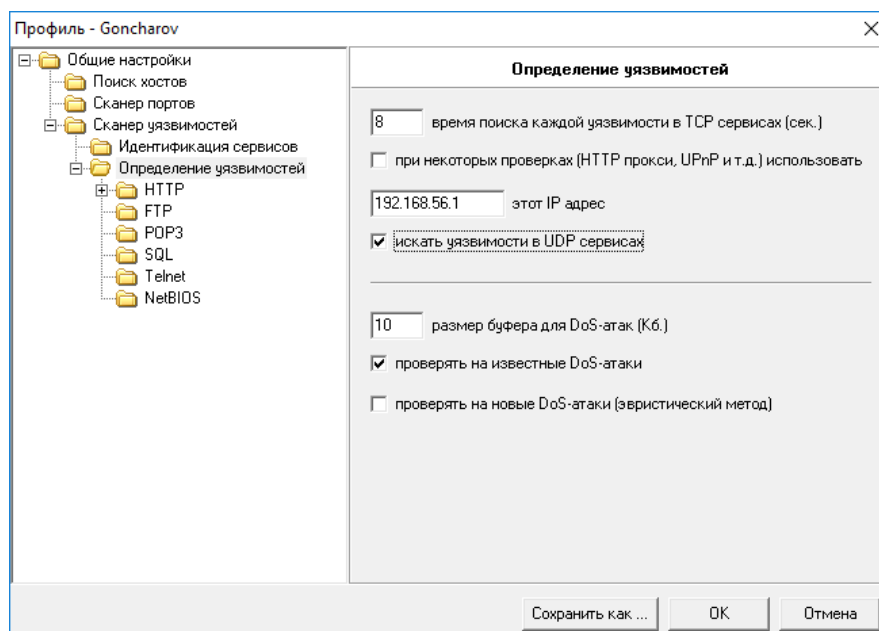
File Edit View Search Terminal Help

mint@mint:~$ sudo xprobe2 -v 192.168.56.101 5.bc.googleusercontent.com.http: Fla
Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@000.nu, ofir@sys-security.com, mede
r@000.nu
[+] Target is 192.168.56.101
[+] Loading modules.
[+] Following modules are loaded:
[x] [1] ping:icmp_ping - ICMP echo discovery module
[x] [2] ping:tcp_ping - TCP-based ping discovery module
[x] [3] ping:udp_ping - UDP-based ping discovery module
[x] [4] infogather:t看l_calc - TCP and UDP based TTL distance calculation
[x] [5] infogather:portscan - TCP and UDP PortScanner
[x] [6] fingerprint:icmp_echo - ICMP Echo request fingerprinting module
[x] [7] fingerprint:icmp_tstamp - ICMP Timestamp request fingerprinting module
[x] [8] fingerprint:icmp_amask - ICMP Address mask request fingerprinting modu
le
[x] [9] fingerprint:icmp_port_unreach - ICMP port unreachable fingerprinting m
odule
[x] [10] fingerprint:tcp_hshake - TCP Handshake fingerprinting module
[x] [11] fingerprint:tcp_rst - TCP RST fingerprinting module
[x] [12] fingerprint:smb - SMB fingerprinting module
[x] [13] fingerprint:snmp - SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 192.168.56.101. Modu
```



```
mint@mint: ~  
File Edit View Search Terminal Help  
[x] [2] ping:tcp_ping - TCP-based ping discovery module  
[x] [3] ping:udp_ping - UDP-based ping discovery module  
[x] [4] infogather:tll_calc - TCP and UDP based TTL distance calculation  
[x] [5] infogather:portscan - TCP and UDP PortScanner  
[x] [6] fingerprint:icmp_echo - ICMP Echo request fingerprinting module  
[x] [7] fingerprint:icmp_tstamp - ICMP Timestamp request fingerprinting module  
[x] [8] fingerprint:icmp_amask - ICMP Address mask request fingerprinting module  
[x] [9] fingerprint:icmp_port_unreach - ICMP port unreachable fingerprinting module  
[x] [10] fingerprint:tcp_hshake - TCP Handshake fingerprinting module  
[x] [11] fingerprint:tcp_rst - TCP RST fingerprinting module  
[x] [12] fingerprint:smb - SMB fingerprinting module  
[x] [13] fingerprint:snmp - SNMPv2c fingerprinting module  
[+] 13 modules registered  
[+] Initializing scan engine  
[+] Running scan engine  
[-] ping:tcp_ping module: no closed/open TCP ports known on 192.168.56.102. Module test failed  
[-] ping:udp_ping module: no closed/open UDP ports known on 192.168.56.102. Module test failed  
[-] No distance calculation. 192.168.56.102 appears to be dead or no ports known  
[+] Host: 192.168.56.102 is down (Guess probability: 0%)  
[+] Cleaning up scan engine  
[+] Modules deinitialized  
[+] Execution completed.  
mint@mint:~$
```

Шаг 5. Перейдите в консоль XSpider. Обратите 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.



Задача1 (Goncharov.prf) - XSpider 7.5 Build 1712

ФайлПравкаВидПрофильСканированиеСкринсОкноXSpider 7.5 by Whack TM

Сканируемые хосты [5]

192.168.56.1 [DESKTOP-1FUKSL2] (12)

192.168.56.100 (255)

192.168.56.102 (64)

192.168.56.2 (249)

192.168.56.101 (128)

Система

Windows 5.1

25 / tcp - smtp

110 / tcp - pop3

119 / tcp - nnrp

123 / udp - NTP

135 / tcp - RPC Windows

137 / udp - NetBIOS-SSN

139 / tcp - NetBIOS

143 / tcp - imap

445 / tcp - Microsoft DS

465 / tcp - Заблокирован

563 / tcp - Заблокирован

587 / tcp - submission

993 / tcp - Заблокирован

995 / tcp - Заблокирован

Доступна информация

Windows 5.1

Описание

Вероятная версия операционной системы : Windows 5.1

СканированиеУязвимостиИстория сканирований

192.168.56.101