

Санкт-Петербургский государственный политехнический университет

Институт компьютерных наук и технологий

Кафедра компьютерных систем и программных технологий

ОТЧЕТ

о лабораторной работе №2

по дисциплине: «Информационная безопасность»

Тема работы: «Утилита для исследования сети и сканер портов Nmap»

Работу выполнил студент

53501/3 *Богданов Н.Е.*

Преподаватель

_____ *Вылегжанина Карина Дмитриевна*

1. Настройка сети

В машине Metasploitable2 выполним следующие команды для настройки сети:

Листинг 1: bash version

```
1 msfadmin@metasploitable:~$ sudo ip addr add 10.0.0.1/24 dev eth1
2 msfadmin@metasploitable:~$ sudo ip link set eth1 up
```

Проверим, что адрес успешно установился:

```
1 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
2 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
3 inet 127.0.0.1/8 scope host lo
4 inet6 ::1/128 scope host
5 valid_lft forever preferred_lft forever
6 2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
   qlen 1000
7 link/ether 08:00:27:9a:98:38 brd ff:ff:ff:ff:ff:ff
8 inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
9 inet6 fe80::a00:27ff:fe9a:9838/64 scope link
10 valid_lft forever preferred_lft forever
11 3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
   qlen 1000
12 link/ether 08:00:27:92:f0:ec brd ff:ff:ff:ff:ff:ff
13 inet 10.0.0.1/24 scope global eth1
14 inet6 fe80::a00:27ff:fe92:f0ec/64 scope link
15 valid_lft forever preferred_lft forever
```

Адрес правильный. Теперь настроим сеть в Kali:

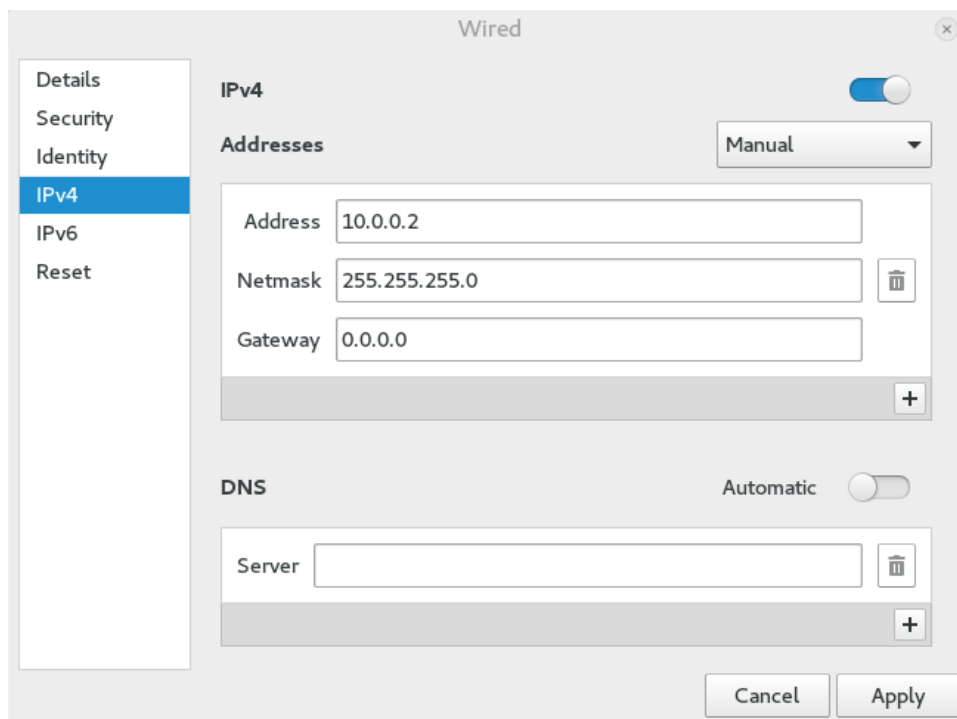


Рис. 1: Установка IPv4-адреса сети

Проверка:

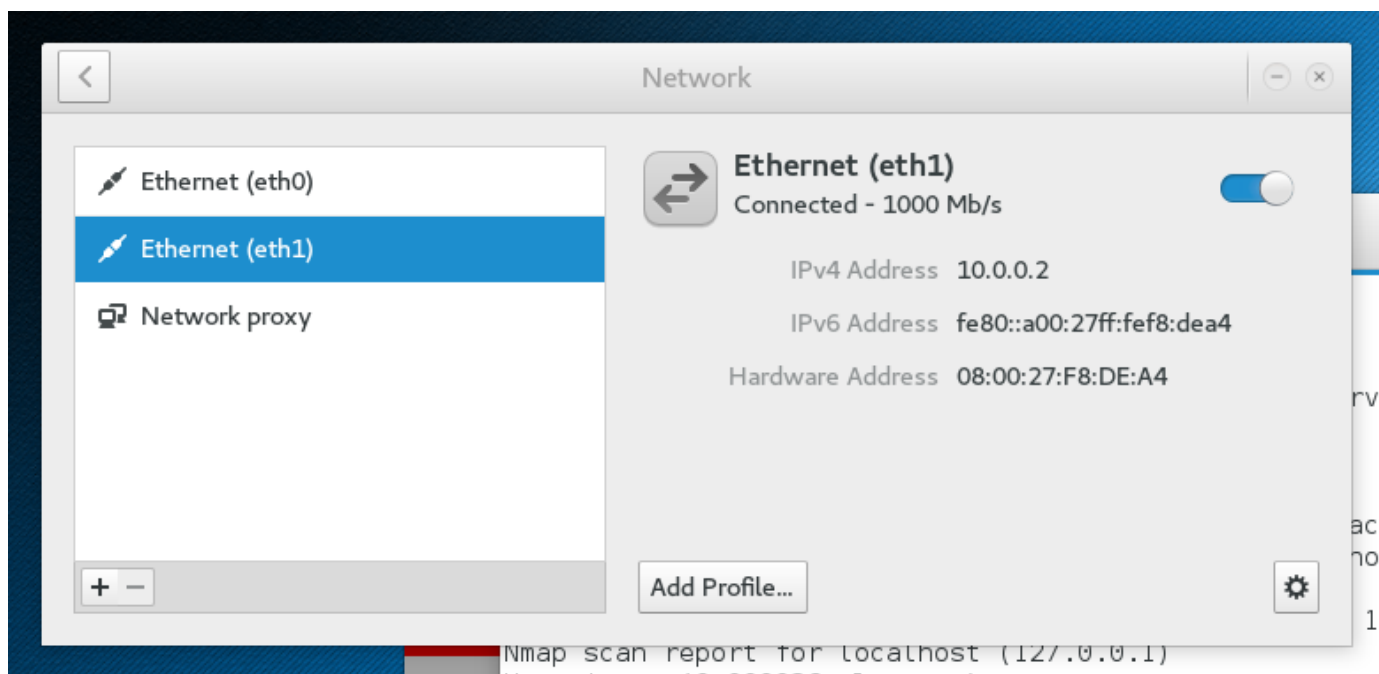


Рис. 2: Состояние интерфейса

Так как в ходе работы придется читать много map-ов, настроим прокрутку в map-страницах (в пейджере по умолчанию, more, нельзя листать вверх).

```
1 root@kali:~# export PAGER=less
```

2. Сканирование сети

Просканируем сеть:

```
1 # nmap -sn 10.0.0.1/24
2
3 Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-20 19:08 EDT
4 Nmap scan report for 10.0.0.1
5 Host is up (0.00023s latency).
6 MAC Address: 08:00:27:92:F0:EC (Oracle VirtualBox virtual NIC)
7 Nmap scan report for 10.0.0.2
8 Host is up.
9 Nmap done: 256 IP addresses (2 hosts up) scanned in 1.98 seconds
```

Просканируем порты:

```
1 root@kali:~# nmap 10.0.0.1
2
3 Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-20 15:34 EDT
4 Nmap scan report for 10.0.0.1
5 Host is up (0.00018s latency).
6 Not shown: 977 closed ports
7 PORT      STATE SERVICE
8 21/tcp    open  ftp
9 22/tcp    open  ssh
10 23/tcp    open  telnet
11 25/tcp    open  smtp
12 53/tcp    open  domain
13 80/tcp    open  http
14 111/tcp   open  rpcbind
```

```

15 139/tcp open netbios-ssn
16 445/tcp open microsoft-ds
17 512/tcp open exec
18 513/tcp open login
19 514/tcp open shell
20 1099/tcp open rmiregistry
21 1524/tcp open ingreslock
22 2049/tcp open nfs
23 2121/tcp open ccproxy-ftp
24 3306/tcp open mysql
25 5432/tcp open postgresql
26 5900/tcp open vnc
27 6000/tcp open X11
28 6667/tcp open irc
29 8009/tcp open ajp13
30 8180/tcp open unknown
31 MAC Address: 08:00:27:92:F0:EC (Oracle VirtualBox virtual NIC)
32
33 Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

```

Анализ версий ПО:

```

1 root@kali:~# nmap -sV 10.0.0.1
2
3 Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-20 15:32 EDT
4 Nmap scan report for 10.0.0.1
5 Host is up (0.00018s latency).
6 Not shown: 977 closed ports
7 PORT      STATE SERVICE      VERSION
8 21/tcp    open  ftp          vsftpd 2.3.4
9 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol
10          2.0)
11 23/tcp    open  telnet       Linux telnetd
12 25/tcp    open  smtp         Postfix smtpd
13 53/tcp    open  domain       ISC BIND 9.4.2
14 80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
15 111/tcp   open  rpcbind      2 (RPC #100000)
16 139/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
17 445/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
18 512/tcp   open  exec         netkit-rsh rexecd
19 513/tcp   open  login?
20 514/tcp   open  tcpwrapped
21 1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
22 1524/tcp  open  shell        Metasploitable root shell
23 2049/tcp  open  nfs          2-4 (RPC #100003)
24 2121/tcp  open  ftp          ProFTPD 1.3.1
25 3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
26 5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
27 5900/tcp  open  vnc          VNC (protocol 3.3)
28 6000/tcp  open  X11          (access denied)
29 6667/tcp  open  irc          Unreal ircd
30 8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
31 8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
32 MAC Address: 08:00:27:92:F0:EC (Oracle VirtualBox virtual NIC)

```

```

32 Service Info: Hosts: metasploitable.localdomain, localhost, irc.
    Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:
    linux_kernel
33
34 Service detection performed. Please report any incorrect results at
    https://nmap.org/submit/ .
35 Nmap done: 1 IP address (1 host up) scanned in 13.54 seconds

```

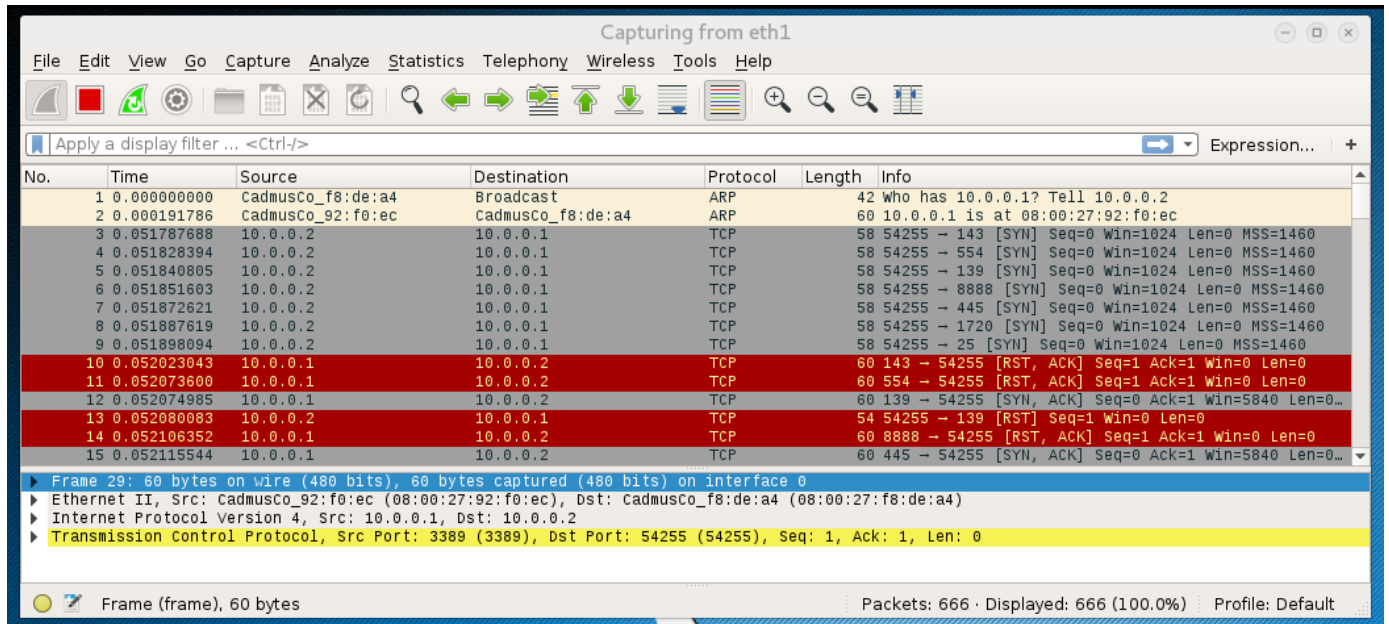


Рис. 3: Анализатор трафика Wireshark

3. Анализ файлов Nmap

Найдем файлы с БД:

```

1 root@kali:~# dpkg -L nmap | grep services
2 /usr/share/nmap/scripts/snmp-win32-services.nse
3 /usr/share/nmap/nmap-services
4 root@kali:~# dpkg -L nmap | grep os-db
5 /usr/share/nmap/nmap-os-db

```

4. Написание своего правила

```

1 root@kali:~# scp pc@desktop:/mnt/win7/Users/pc/Documents/Study/
    Networks_new/Networks_10_11.zip .
2 pc@desktop's password:
3 Networks_10_11.zip                                100%   55KB   55.1KB/s
    00:01
4 root@kali:~# unzip Networks_10_11.zip

```

```

1 root@kali:~/Aleksyuk/CourseClient# ./main
2 Please enter the command: Hi
3 You need to login first (AwesomeWallet 0.1)

```

Сделаем бекап файла с описанием отпечатков

```
1 root@kali:~/pc/CourseClient# sudo cp /usr/share/nmap/nmap-service-  
  probes /usr/share/nmap/nmap-service-probes.backup
```

Напишем правило:

```
1 root@kali:~# cat probe.txt  
2 Probe TCP AwesomeWallet q|\x02Hi|  
3 rarity 1  
4 ports 5004  
5 match wallet m/^You need to login first \((\w*) ([\d.]*)\) / p/$1/ v/  
  $2/
```

Проверим работу регулярного выражения в Python:

```
1 root@kali:~# python3  
2 Python 3.5.1+ (default, Jan 13 2016, 15:09:18)  
3 [GCC 5.3.1 20160101] on linux  
4 Type "help", "copyright", "credits" or "license" for more information  
5 >>> str = "You need to login first (AwesomeWallet 0.1)"  
6 >>> import re  
7 >>> p = re.compile(r"^You need to login first \((\w*) ([\d.]*)\)")  
8 >>> m = p.match(str)  
9 >>> print(m)  
10 <_sre.SRE_Match object; span=(0, 43), match='You need to login first  
   (AwesomeWallet 0.1)'  
11 >>> m.group()  
12 'You need to login first (AwesomeWallet 0.1)'  
13 >>> m.groups()  
14 ('AwesomeWallet', '0.1')  
15 >>> exit()
```

Добавим правило:

```
1 root@kali:~# cat probe.txt >> /usr/share/nmap/nmap-service-probes
```

Результат работы nmap:

```
1 root@kali:~# nmap localhost -p 5004 -sV  
2  
3 Starting Nmap 7.01 ( https://nmap.org ) at 2016-03-20 18:24 EDT  
4 Nmap scan report for localhost (127.0.0.1)  
5 Host is up (0.000036s latency).  
6 Other addresses for localhost (not scanned): ::1  
7 PORT      STATE SERVICE VERSION  
8 5004/tcp  open  wallet  AwesomeWallet 0.1  
9  
10 Service detection performed. Please report any incorrect results at  
   https://nmap.org/submit/ .  
11 Nmap done: 1 IP address (1 host up) scanned in 6.52 seconds
```

По выводу сервера видно, что было произведено подключение и был отправлен тестовый запрос

```
1 root@kali:~/pc/Course# ./main  
2 Waiting  
3 Connection 4  
4 Waiting
```

```
5 Worker for 4 is up
6 Receiving message with length 2
7 Received Hi
8 Receiving message with length 2
9 Received
10 Receiving message with length 2
11 Received
12 ERROR writing to socket: Broken pipe
```

<https://nmap.org/book/vscan-fileformat.html>