

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»  
(СПбГУТ)

---

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

**Лабораторная работа №2**

Выполнили студенты группы ИКТЗ-83:

Громов А.А., Миколаени М.С., Мазеин Д.С.

(Ф.И.О., № группы)

\_\_\_\_\_  
(подпись)

Проверил:

Казанцев А.А.

(уч. степень, уч. звание, Ф.И.О.)

\_\_\_\_\_  
(подпись)

Санкт-Петербург

2021

## Часть 1 - Honeypot, Nmap

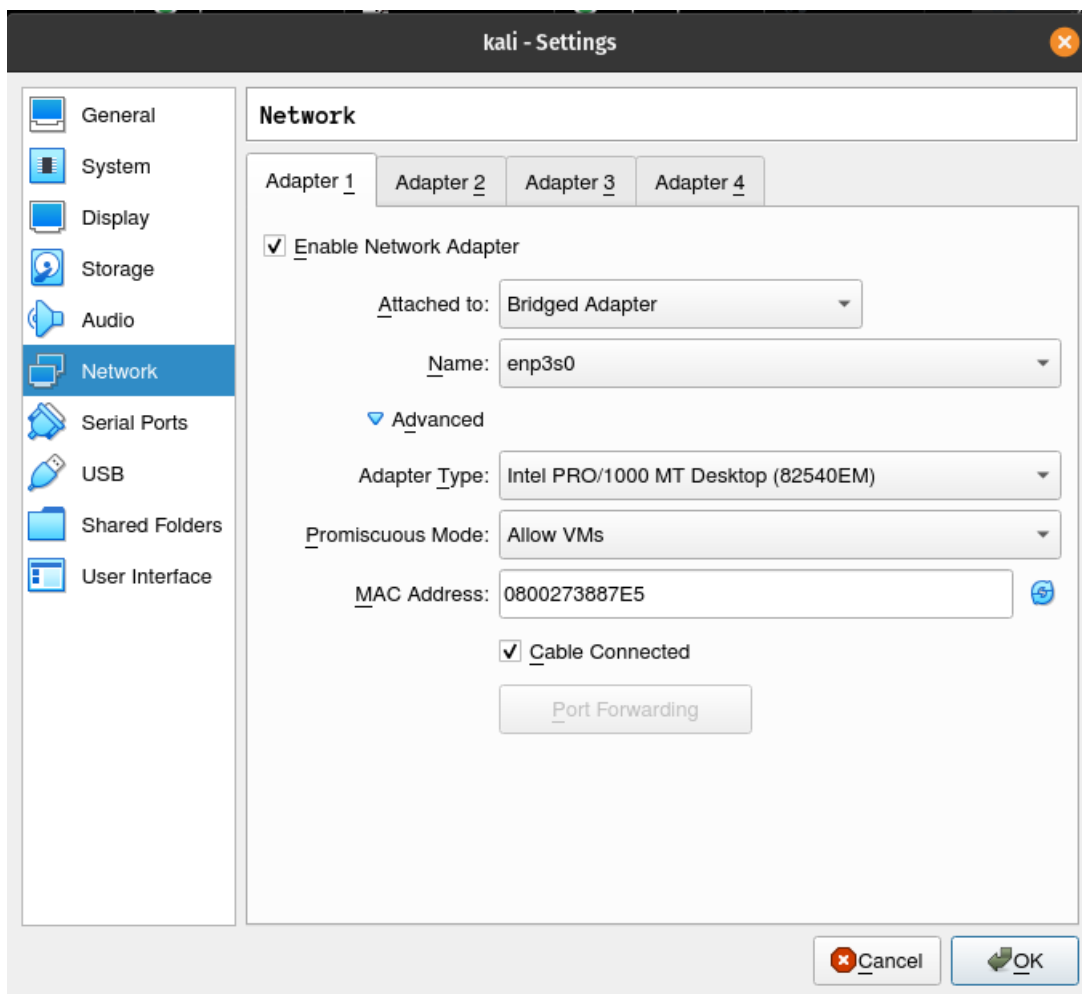


Рис. 1 Настройка сетевого адаптера для виртуальной машины.

```
iktz-83@iktz83: ~  
iktz-83@iktz83: ~  
iktz-83@iktz83:~$ ifconfig  
Command 'ifconfig' not found, but can be installed with:  
sudo apt install net-tools  
iktz-83@iktz83:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:b0:7c:91 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.0.97/25 brd 192.168.0.127 scope global dynamic noprefixroute enp0s3  
        valid_lft 6468sec preferred_lft 6468sec  
    inet6 fe80::4fd5:c463:f1e9:38f0/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
iktz-83@iktz83:~$ ^C  
iktz-83@iktz83:~$
```

Рис. 2 Определение ip адреса сервера.

```
File Actions Edit View Help
iktz-83@kali:~ iktz-83@kali:~ iktz-83@kali:~

Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
1900/tcp  open  upnp
20005/tcp open  btx
MAC Address: B0:BE:76:44:5A:EC (Tp-link Technologies)

Nmap scan report for 192.168.0.4
Host is up (0.0015s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
62078/tcp open  iphone-sync
MAC Address: F2:BD:DE:F3:E4:DE (Unknown)

Nmap scan report for 192.168.0.30
Host is up (0.0013s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
5900/tcp  open  vnc
9091/tcp  open  xmltec-xmlmail
MAC Address: B8:27:EB:91:FD:35 (Raspberry Pi Foundation)

Nmap scan report for 192.168.0.33
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.0.33 are closed
MAC Address: D8:50:E6:4C:30:28 (Asustek Computer)

Nmap scan report for 192.168.0.97
Host is up (0.00047s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:B0:7C:91 (Oracle VirtualBox virtual NIC)
```

Рис. 3 Сканируем сеть для нахождения хостов и открытых порты на них.

```
File Actions Edit View Help
iktz-83@kali:~ iktz-83@kali:~ iktz-83@kali:~

iktz-83@kali ~$ sudo nmap -sP -n 192.168.0.0/16
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 14:53 MSK
Nmap scan report for 192.168.0.1
Host is up (0.00053s latency).
MAC Address: B0:BE:76:44:5A:EC (Tp-link Technologies)
Nmap scan report for 192.168.0.4
Host is up (0.11s latency).
MAC Address: F2:BD:DE:F3:E4:DE (Unknown)
Nmap scan report for 192.168.0.30
Host is up (0.00090s latency).
MAC Address: B8:27:EB:91:FD:35 (Raspberry Pi Foundation)
Nmap scan report for 192.168.0.33
Host is up (0.00051s latency).
MAC Address: D8:50:E6:4C:30:28 (Asustek Computer)
Nmap scan report for 192.168.0.85
Host is up (0.056s latency).
MAC Address: A8:34:6A:2B:9A:CA (Samsung Electronics)
Nmap scan report for 192.168.0.97
Host is up (0.00024s latency).
MAC Address: 08:00:27:B0:7C:91 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.51
Host is up.
```

Рис. 4 Сканируем сеть для нахождения хостов без портов.

```
valid_ttl forever preferred_ttl forever
iktz-83@kali ~$ ping 192.168.0.97
PING 192.168.0.97 (192.168.0.97) 56(84) bytes of data:
64 bytes from 192.168.0.97: icmp_seq=1 ttl=64 time=0.311 ms
64 bytes from 192.168.0.97: icmp_seq=2 ttl=64 time=0.748 ms
64 bytes from 192.168.0.97: icmp_seq=3 ttl=64 time=0.308 ms
64 bytes from 192.168.0.97: icmp_seq=4 ttl=64 time=0.415 ms
64 bytes from 192.168.0.97: icmp_seq=5 ttl=64 time=0.594 ms
64 bytes from 192.168.0.97: icmp_seq=6 ttl=64 time=0.517 ms
64 bytes from 192.168.0.97: icmp_seq=7 ttl=64 time=0.419 ms
^C
--- 192.168.0.97 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6184ms
rtt min/avg/max/mdev = 0.308/0.473/0.748/0.147 ms
iktz-83@kali ~$
```

Рис. 5 Проверяем наличие отклика от сервера.

```
iktz-83@kali ~$ sudo nmap -sT -v 192.168.0.97
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 14:59 MSK
Initiating ARP Ping Scan at 14:59
Scanning 192.168.0.97 [1 port]
Completed ARP Ping Scan at 14:59, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:59
Completed Parallel DNS resolution of 1 host. at 14:59, 0.01s elapsed
Initiating Connect Scan at 14:59
Scanning 192.168.0.97 [1000 ports]
Discovered open port 80/tcp on 192.168.0.97
Completed Connect Scan at 14:59, 0.09s elapsed (1000 total ports)
Nmap scan report for 192.168.0.97
Host is up (0.00072s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:B0:7C:91 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```

Рис. 6 Сканируем ip-адрес на наличие открытых портов с помощью TCP connect scan.

```
iktz-83@kali ~$ sudo nmap -sF -v 192.168.0.97
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 15:09 MSK
Initiating ARP Ping Scan at 15:09
Scanning 192.168.0.97 [1 port]
Completed ARP Ping Scan at 15:09, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:09
Completed Parallel DNS resolution of 1 host. at 15:09, 0.01s elapsed
Initiating FIN Scan at 15:09
Scanning 192.168.0.97 [1000 ports]
Completed FIN Scan at 15:09, 1.33s elapsed (1000 total ports)
Nmap scan report for 192.168.0.97
Host is up (0.00011s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open|filtered http
MAC Address: 08:00:27:B0:7C:91 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
Raw packets sent: 1002 (40.068KB) | Rcvd: 1000 (39.988KB)
```

Рис. 7 Сканируем ip-адрес на наличие открытых портов с помощью FIN scan.

```
iktz-83@kali ~$ sudo nmap -sX -v 192.168.0.97
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 15:10 MSK
Initiating ARP Ping Scan at 15:10
Scanning 192.168.0.97 [1 port]
Completed ARP Ping Scan at 15:10, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:10
Completed Parallel DNS resolution of 1 host. at 15:10, 0.01s elapsed
Initiating XMAS Scan at 15:10
Scanning 192.168.0.97 [1000 ports]
Completed XMAS Scan at 15:10, 1.25s elapsed (1000 total ports)
Nmap scan report for 192.168.0.97
Host is up (0.00010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open|filtered http
MAC Address: 08:00:27:B0:7C:91 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds
Raw packets sent: 1002 (40.068KB) | Rcvd: 1000 (39.988KB)
iktz-83@kali ~$
```

Рис. 8 Сканируем ip-адрес на наличие открытых портов с помощью Xmas scan.

```

iktz-83@kali ~$ sudo nmap -sN -v 192.168.0.97
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 15:10 MSK
Initiating ARP Ping Scan at 15:10
Scanning 192.168.0.97 [1 port]
Completed ARP Ping Scan at 15:10, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:10
Completed Parallel DNS resolution of 1 host. at 15:10, 0.01s elapsed
Initiating NULL Scan at 15:10
Scanning 192.168.0.97 [1000 ports]
Completed NULL Scan at 15:10, 1.27s elapsed (1000 total ports)
Nmap scan report for 192.168.0.97
Host is up (0.00021s latency).
Not shown: 999 closed ports
PORT      STATE      SERVICE
80/tcp    open|filtered http
MAC Address: 08:00:27:B0:7C:91 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
Raw packets sent: 1002 (40.068KB) | Rcvd: 1000 (39.988KB)
iktz-83@kali ~$

```

Рис. 9 Сканируем ip-адрес на наличие открытых портов с помощью Null scan.

```

iktz-83@kali:~$ sudo nmap -sO -v 192.168.0.97
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 15:11 MSK
Initiating ARP Ping Scan at 15:11
Scanning 192.168.0.97 [1 port]
Completed ARP Ping Scan at 15:11, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:11
Completed Parallel DNS resolution of 1 host. at 15:11, 0.01s elapsed
Initiating IPProto Scan at 15:11
Scanning 192.168.0.97 [256 ports]
Increasing send delay for 192.168.0.97 from 0 to 5 due to max_successful_ryno increase to 4
Increasing send delay for 192.168.0.97 from 5 to 10 due to max_successful_ryno increase to 5
Increasing send delay for 192.168.0.97 from 10 to 20 due to max_successful_ryno increase to 6
Discovered open port 6/tcp on 192.168.0.97
Increasing send delay for 192.168.0.97 from 20 to 40 due to 11 out of 15 dropped probes since last increase.
Increasing send delay for 192.168.0.97 from 40 to 80 due to max_successful_ryno increase to 7
IPProto Scan Timing: About 38.67% done; ETC: 15:12 (0:00:49 remaining)
Increasing send delay for 192.168.0.97 from 80 to 160 due to max_successful_ryno increase to 8
Increasing send delay for 192.168.0.97 from 160 to 320 due to max_successful_ryno increase to 9
Increasing send delay for 192.168.0.97 from 320 to 640 due to max_successful_ryno increase to 10
Increasing send delay for 192.168.0.97 from 640 to 1000 due to 11 out of 23 dropped probes since last increase.
IPProto Scan Timing: About 45.13% done; ETC: 15:13 (0:01:14 remaining)
Warning: 192.168.0.97 giving up on port because retransmission cap hit (10).
Discovered open port 1/tcp on 192.168.0.97
IPProto Scan Timing: About 68.29% done; ETC: 15:14 (0:00:58 remaining)
IPProto Scan Timing: About 79.62% done; ETC: 15:14 (0:00:42 remaining)
Stats: 0:03:37 elapsed; 0 hosts completed (1 up), 1 undergoing IPProto Scan
IPProto Scan Timing: About 98.72% done; ETC: 15:15 (0:00:03 remaining)
Discovered open port 17/tcp on 192.168.0.97
Completed IPProto Scan at 15:16, 286.92s elapsed (256 total ports)
Nmap scan report for 192.168.0.97
Host is up (0.00050s latency).
Not shown: 250 closed protocols
PROTOCOL STATE      SERVICE
1          open          icmp
2          open|filtered igmp
6          open          tcp
17         open          udp
103        open|filtered pim
136        open|filtered udplite
MAC Address: 08:00:27:B0:7C:91 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 287.10 seconds
Raw packets sent: 878 (17.724KB) | Rcvd: 265 (12.712KB)
iktz-83@kali ~$

```

Рис. 10 Сканируем ip-адрес на наличие открытых портов с помощью IP protocol scan.

```

iktz-83@kali ~$ sudo nmap -sA -v 192.168.0.97
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 15:18 MSK
Initiating ARP Ping Scan at 15:18
Scanning 192.168.0.97 [1 port]
Completed ARP Ping Scan at 15:18, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:18
Completed Parallel DNS resolution of 1 host. at 15:18, 0.01s elapsed
Initiating ACK Scan at 15:18
Scanning 192.168.0.97 [1000 ports]
Completed ACK Scan at 15:18, 0.10s elapsed (1000 total ports)
Nmap scan report for 192.168.0.97
Host is up (0.00015s latency).
All 1000 scanned ports on 192.168.0.97 are unfiltered
MAC Address: 08:00:27:B0:7C:91 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
Raw packets sent: 1001 (40.028KB) | Rcvd: 1001 (40.028KB)
iktz-83@kali ~$

```

Рис. 11 Сканируем ip-адрес на наличие открытых портов с помощью TCP ACK scan.

```

iktz-83@kali ~$ sudo nmap -sW -v 192.168.0.97
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 15:18 MSK
Initiating ARP Ping Scan at 15:18
Scanning 192.168.0.97 [1 port]
Completed ARP Ping Scan at 15:18, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:18
Completed Parallel DNS resolution of 1 host. at 15:18, 0.01s elapsed
Initiating Window Scan at 15:18
Scanning 192.168.0.97 [1000 ports]
Completed Window Scan at 15:18, 0.11s elapsed (1000 total ports)
Nmap scan report for 192.168.0.97
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.0.97 are closed
MAC Address: 08:00:27:B0:7C:91 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
Raw packets sent: 1001 (40.028KB) | Rcvd: 1001 (40.028KB)
iktz-83@kali ~$

```

Рис. 12 Сканируем ip-адрес на наличие открытых портов с помощью TCP Window scan.

```

iktz-83@kali ~$ sudo nmap -sR -v 192.168.0.97
WARNING: -sR is now an alias for -sV and activates version detection as well as RPC scan.
Warning: The -sR option is deprecated. Please use -sV
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 15:21 MSK
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 15:21
Scanning 192.168.0.97 [1 port]
Completed ARP Ping Scan at 15:21, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:21
Completed Parallel DNS resolution of 1 host. at 15:21, 0.01s elapsed
Initiating SYN Stealth Scan at 15:21
Scanning 192.168.0.97 [1000 ports]
Discovered open port 80/tcp on 192.168.0.97
Completed SYN Stealth Scan at 15:21, 0.11s elapsed (1000 total ports)
Initiating Service scan at 15:21
Scanning 1 service on 192.168.0.97
Completed Service scan at 15:22, 6.06s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.0.97.
Initiating NSE at 15:22
Completed NSE at 15:22, 0.01s elapsed
Initiating NSE at 15:22
Completed NSE at 15:22, 0.00s elapsed
Nmap scan report for 192.168.0.97
Host is up (0.00012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 08:00:27:B0:7C:91 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.89 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.032KB)
iktz-83@kali ~$

```

Рис. 13 Сканируем ip-адрес на наличие открытых портов с помощью Version detection.



```
iktz-83@kali ~$ sudo nmap -O 192.168.0.97
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 15:25 MSK
Nmap scan report for 192.168.0.97
Host is up (0.00049s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:80:7C:91 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6, Linux 5.0 - 5.3
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
```

Рис. 14 Сканируем ip-адрес для определения операционной системы.

## Часть 2 - WEB APPLICATION FIREWALL

```
gromov@pop-os ~$ sudo nmap -sX -v 192.168.0.51
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-06 16:24 MSK
Initiating ARP Ping Scan at 16:24
Scanning 192.168.0.51 [1 port]
Completed ARP Ping Scan at 16:24, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:24
Completed Parallel DNS resolution of 1 host. at 16:24, 0.02s elapsed
Initiating XMAS Scan at 16:24
Scanning 192.168.0.51 [1000 ports]
Completed XMAS Scan at 16:24, 21.10s elapsed (1000 total ports)
Nmap scan report for 192.168.0.51
Host is up (0.00023s latency).
All 1000 scanned ports on 192.168.0.51 are open|filtered
MAC Address: 08:00:27:38:87:E5 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.29 seconds
Raw packets sent: 2001 (80.028KB) | Rcvd: 1 (28B)
```

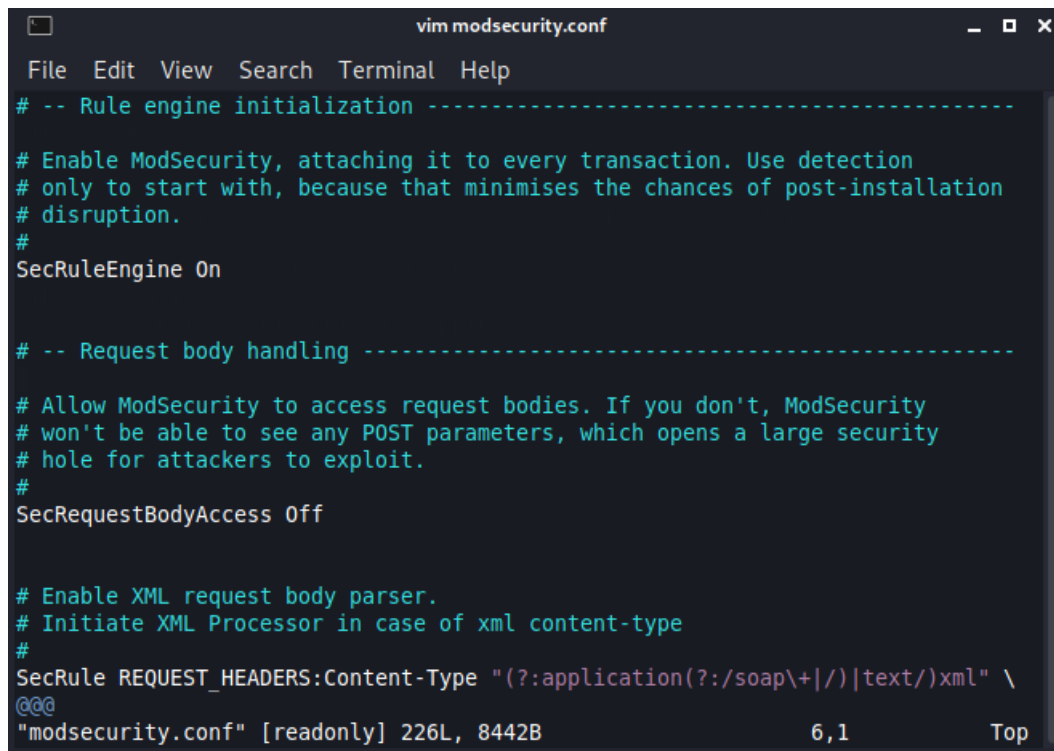
Рис. 15 Неудачное сканирование ip-адреса на наличие открытых портов с помощью Xmas scan, так как на сервере настроен iptables.

```
iktz-83@kali ~$ sudo ls -la /var/log/apache2
total 8
drwxr-x--- 2 root adm 4096 Apr 25 05:18 .
drwxr-xr-x 18 root root 4096 May 6 15:41 ..
-rw-r----- 1 root adm 0 Apr 25 05:18 access.log
-rw-r----- 1 root adm 0 Apr 25 05:18 error.log
-rw-r----- 1 root adm 0 Apr 25 05:18 other_vhosts_access.log
```

Рис. 16 Проверяем новый лог-файл.

```
iktz-83@kali /etc/modsecurity$ ls -la
total 84
drwxr-xr-x 3 root root 4096 May 6 16:26 .
drwxr-xr-x 162 root root 12288 May 6 16:26 ..
drwxr-xr-x 2 root root 4096 May 6 16:26 crs
-rw-r--r-- 1 root root 8452 Dec 10 21:14 modsecurity.conf-recommended
-rw-r--r-- 1 root root 53146 Dec 4 2018 unicode.mapping
iktz-83@kali /etc/modsecurity$ mv modsecurity.conf-recommended modsecurity.conf
mv: cannot move 'modsecurity.conf-recommended' to 'modsecurity.conf': Permission denied
iktz-83@kali /etc/modsecurity$ sudo mv modsecurity.conf-recommended modsecurity.conf
iktz-83@kali /etc/modsecurity$ ls
crs modsecurity.conf unicode.mapping
iktz-83@kali /etc/modsecurity$
```

Рис. 17 Переименовываем конфигурационный файл apache2-mod-security2.



```
vim modsecurity.conf
File Edit View Search Terminal Help
# -- Rule engine initialization -----
# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
SecRuleEngine On

# -- Request body handling -----
# Allow ModSecurity to access request bodies. If you don't, ModSecurity
# won't be able to see any POST parameters, which opens a large security
# hole for attackers to exploit.
#
SecRequestBodyAccess Off

# Enable XML request body parser.
# Initiate XML Processor in case of xml content-type
#
SecRule REQUEST_HEADERS:Content-Type "(?:application(?:/soap\+|/)|text/)xml" \
@@@
"modsecurity.conf" [readonly] 226L, 8442B 6,1 Top
```

Рис. 18 Редактируем конфигурацию apache2-mod-security2 под наши нужды.

## Вывод

В данной лабораторной работе мы научились сканировать ip-адреса на наличие открытых портов различными методами. Также произвели протестировали сервер на уязвимости, после настройки iptables(файервола) на нем.