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)*
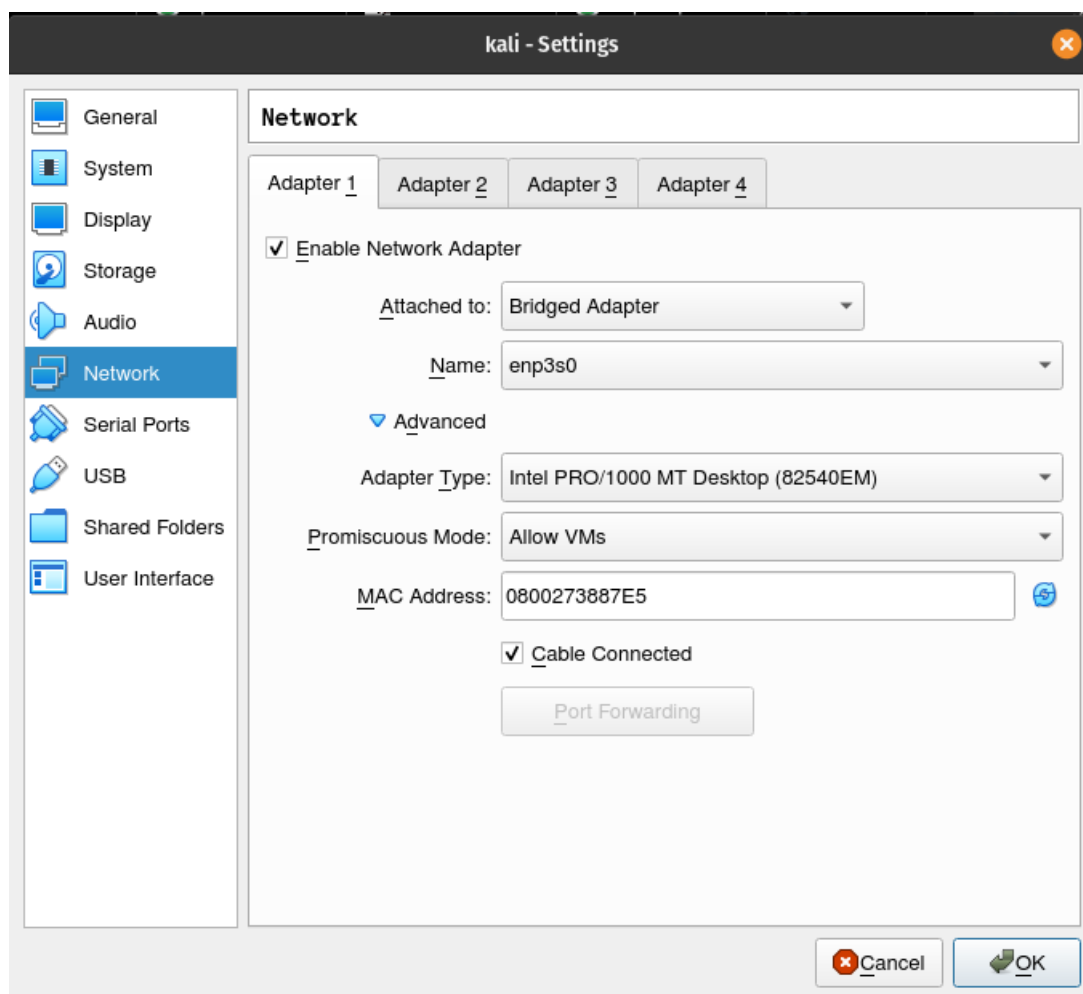
Санкт-Петербург

2021

Часть 1 - Honeypot, Nmap

Рис. 1

Рис. 2

```
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


```
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

```
  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

```
  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

```
  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

```
  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

```
 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

```
                                  iktz-83@kali:~                                  _ □ ×
File   Actions   Edit   View   Help
     iktz-83@kali:~         ⊠        iktz-83@kali:~       ⊠      iktz-83@kali:~      ⊠
 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_tryno increase to 4
Increasing send delay for 192.168.0.97 from 5 to 10 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.0.97 from 10 to 20 due to max_successful_tryno increase to 6
Discovered open port 6/ip 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_tryno 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_tryno increase to 8
Increasing send delay for 192.168.0.97 from 160 to 320 due to max_successful_tryno increase to 9
Increasing send delay for 192.168.0.97 from 320 to 640 due to max_successful_tryno 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/ip 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/ip 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

```
   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

```
 x 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

```
   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

```
 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:B0:7C: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

Часть 2 - WEB APLICATION FIREWALL

Рис. 15

Рис. 16

Рис. 17

Рис. 18