Лабораторная работа № 2

Тема: пассивные сетевые атаки.

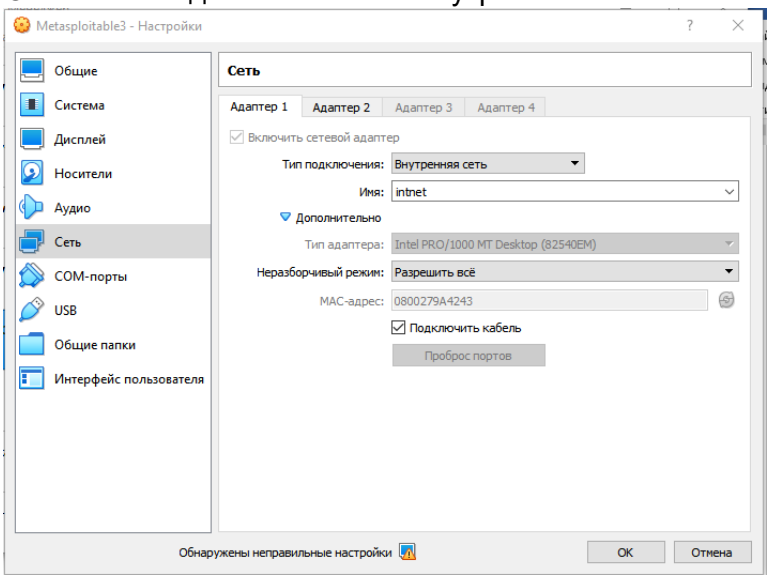
Оборудование:
- компьютер с установленной программой Virtual box или аналогичной;
- дистрибутив Kali Linux;
- дистрибутив metasploitable3.

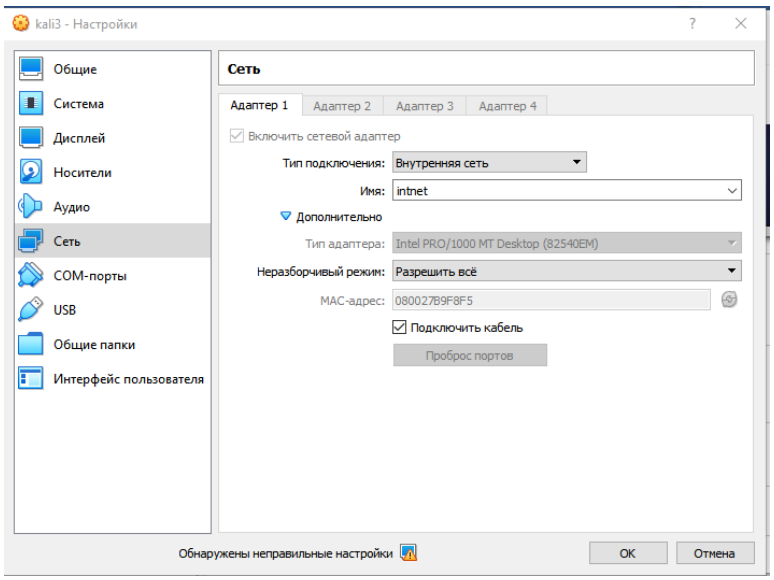
Задание:

1. Ознакомиться со следующими статьями Уголовного Кодекса РК:

Статья 205. Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций.
Статья 206. Неправомерные уничтожение или модификация информации.
Статья 207. Нарушение работы информационной системы или сетей телекоммуникаций.
Статья 208. Неправомерное завладение информацией.
Статья 210. Создание, использование или распространение вредоносных компьютерных программ и программных продуктов.
Статья 211. Неправомерное распространение электронных информационных ресурсов ограниченного доступа.

2. Подготовьте испытательный стенд:
Установите на виртуальную машину Kali Linux 2023 и Metasploitable3.
Обе машины должны быть во внутренней сети:





Настройте сетевые интерфейсы, для каждой машины выполните шаги:
Посмотрите список сетевых интерфейсов:
ip -a
Включите сетевой интерфейс снова с помощью команды:
sudo ifconfig eth0 up
Настройте IP-адрес с помощью команды:
sudo ifconfig eth0 <IP-адрес> netmask <маска подсети>
Включите сетевой интерфейс снова с помощью команды:
sudo ifconfig eth0 up
Проверьте настройки сетевого интерфейса снова с помощью команды:
ifconfig eth0
Вы должны увидеть новый IP-адрес, который вы настроили для выбранного сетевого интерфейса.

Например:

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault 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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:b9:f8:f5 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::60a4:fc7:6f04:8277/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 down

┌──(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 10.10.0.20 netmask 255.255.255.0

┌──(kali㉿kali)-[~]
└─$ sudo ifconfig eth0 up

┌──(kali㉿kali)-[~]
└─$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.0.20  netmask 255.255.255.0  broadcast 10.10.0.255
        ether 08:00:27:b9:f8:f5  txqueuelen 1000  (Ethernet)
        RX packets 938  bytes 109156 (106.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 902  bytes 84320 (82.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Проверьте связь между машинами командой ping:

```
vagrant@metasploitable3-ub1404:~$ ping 10.10.0.20
PING 10.10.0.20 (10.10.0.20) 56(84) bytes of data.
64 bytes from 10.10.0.20: icmp_seq=1 ttl=64 time=1.59 ms
64 bytes from 10.10.0.20: icmp_seq=2 ttl=64 time=1.07 ms
64 bytes from 10.10.0.20: icmp_seq=3 ttl=64 time=2.35 ms
64 bytes from 10.10.0.20: icmp_seq=4 ttl=64 time=1.95 ms
64 bytes from 10.10.0.20: icmp_seq=5 ttl=64 time=1.11 ms
64 bytes from 10.10.0.20: icmp_seq=6 ttl=64 time=2.02 ms
64 bytes from 10.10.0.20: icmp_seq=7 ttl=64 time=1.98 ms
64 bytes from 10.10.0.20: icmp_seq=8 ttl=64 time=1.89 ms
64 bytes from 10.10.0.20: icmp_seq=9 ttl=64 time=1.46 ms
```

3. В Kali Linux просканируйте локальную сеть на наличие активных хостов с помощью nmap, используйте различные методы сканирования.

4. Используя утилиту nmap, просканируйте порты активного хоста, попробуйте различные методы сканирования. Захватите трафик в Wire Shark во время сканирования и проследите за соответствующими запросами.

5. Определите версии служб «слушающих» открытые порты.

6. Определите версию ОС исследуемого хоста.

7. Создайте еще одну виртуальную машину Ubuntu Server, на которой запустите несколько сервисов (ngnix, ssh, postfix). Повторите предыдущие пункты.

8. Выполните сканирование сети и сканирование портов в программе с графическим интерфейсом, например Legion.