

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Прикладные информационные технологии» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОЙ РАБОТЫ №1**

**В РАМКАХ ДИСЦИПЛИНЫ «БЕЗОПАСНОСТЬ ПРИКЛАДНЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ»**

Выполнил:

Студент 2-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Оглавление

[Подготовительный этап 3](#_Toc161307990)

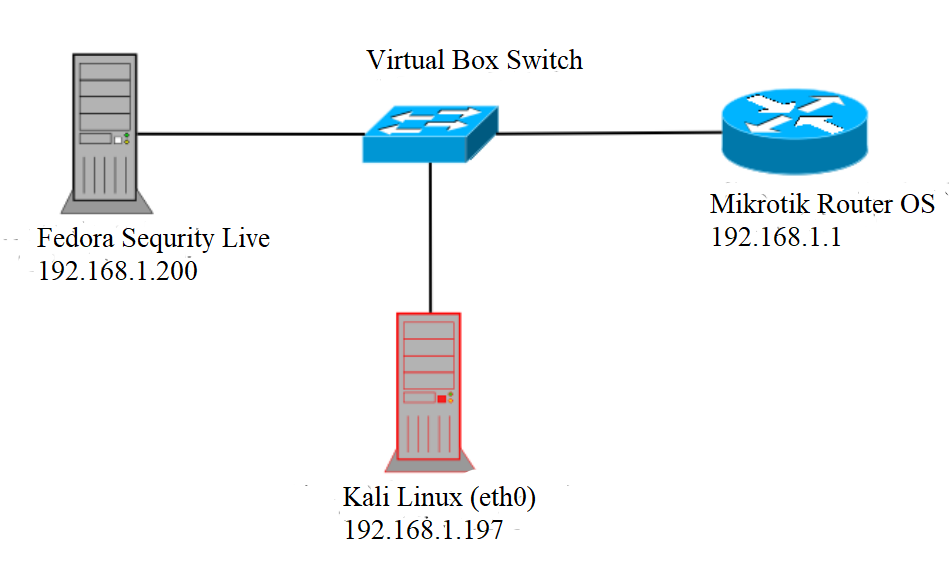
[Обнаружение узлов на локальном уровне 4](#_Toc161307991)

[Осуществление атаки ARP poisoning. Перехват данных аутентификации в прикладном протоколе. 4](#_Toc161307992)

[Осуществление атаки DHCP 6](#_Toc161307993)

# Подготовительный этап

Для выполнения практической работы будет использоваться следующая конфигурация



Компьютер злоумышленника – дистрибутив для тестирования безопасности Kali Linux 2023.4

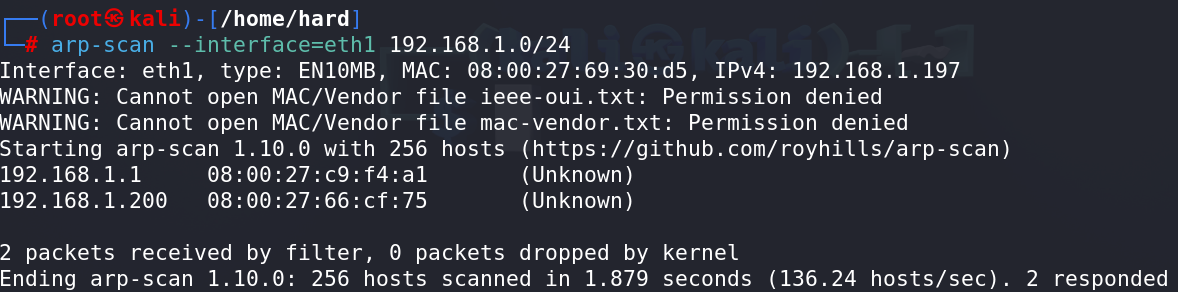
Маршрутиатор – Mikrotik RouterOS

Пользователь локальной сети – Fedora Security Live (FSL)

На всех VM сетевые интерфейсы находятся в режиме Internal Net

# Обнаружение узлов на локальном уровне

С помощью программы ARP-SCAN с рабочего места злоумышленника выявите узлы в локальной сети, запишите их MAC-адреса.



# Осуществление атаки ARP poisoning. Перехват данных аутентификации в прикладном протоколе.

Для осуществления MITM-атак проверьте активацию IP-forwarding в FSL.

# cat /proc/sys/net/ipv4/ip\_forward

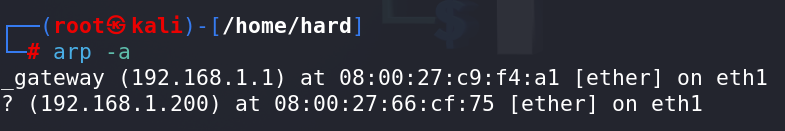
Если значение в 0, то включите ip-forwarding командой:

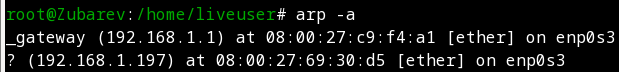
# echo 1 > /proc/sys/net/ipv4/ip\_forward

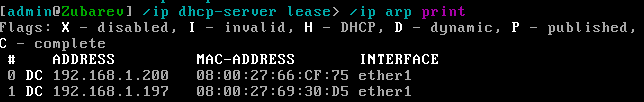
Проверьте записи в arp-таблице всех трех хостов командами

# arp -­a

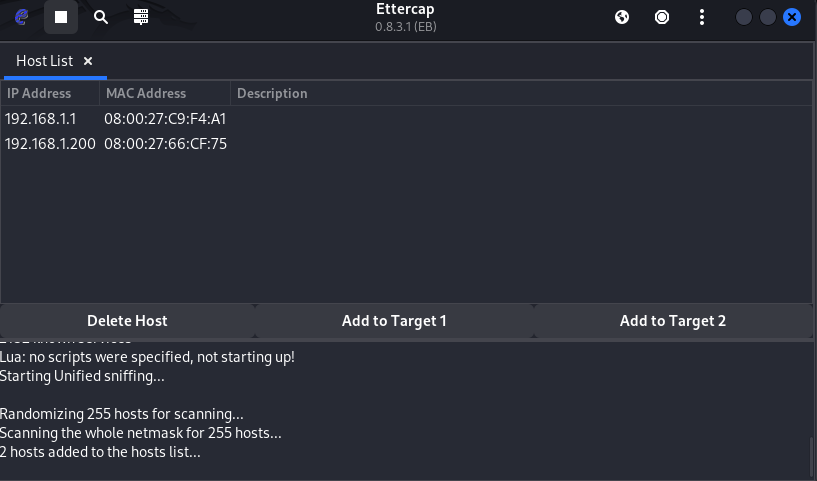
Mikrotik> ip arp print



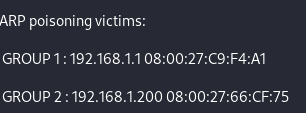




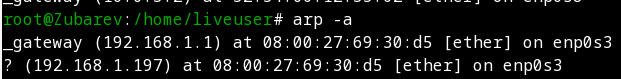
После сканирования в Host list просмотрите выявленные узлы:

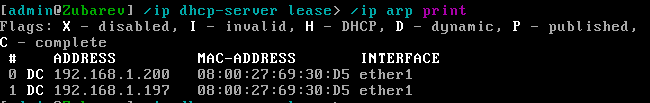


Добавьте адрес шлюза в Target 1, а адрес Tiny Core в Target 2. В меню MITM выберите атаку ARP poisoning. Выберите опцию Sniff remote connections.

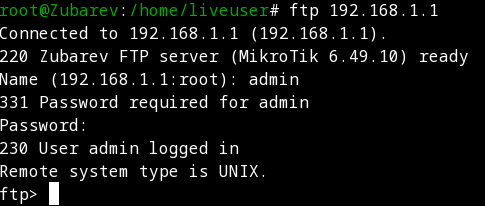


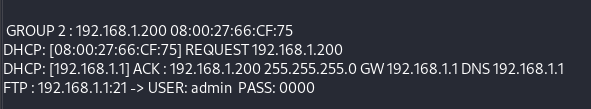
Снова проверим содержимое ARP-таблиц:





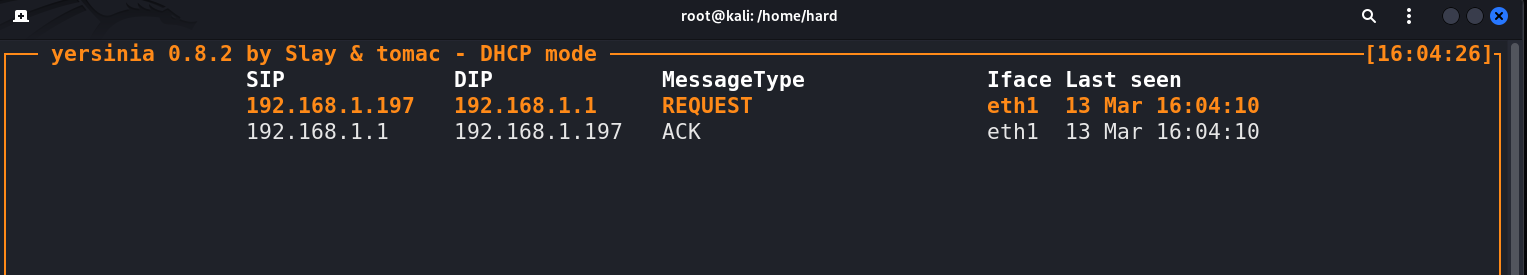
Осуществим подключение с Пользовательского ПК FSL на FTP-сервер маршрутизатора Mikrotik. На Kali Linux проверяем перехваченные данные:

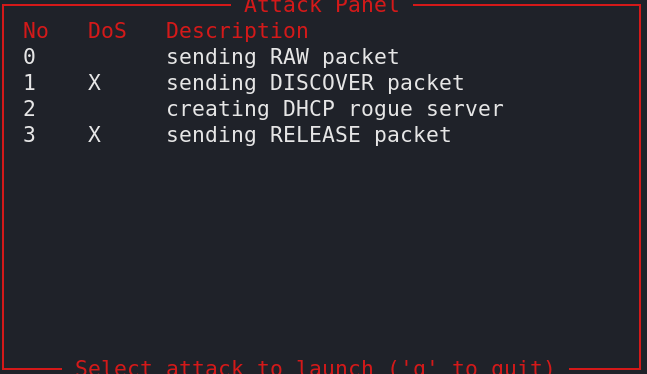




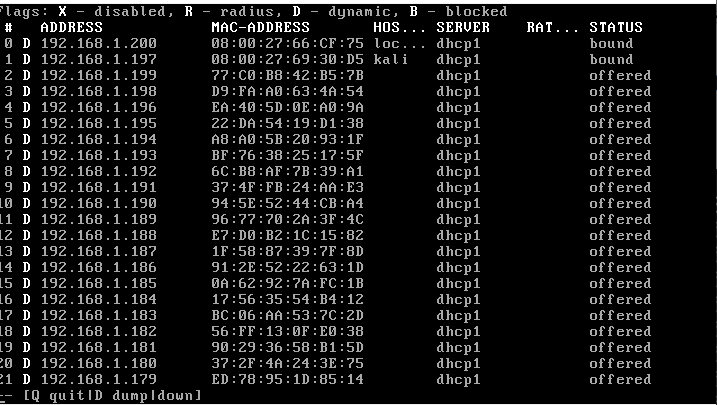
# Осуществление атаки DHCP

Требуется нарушить работу существующего DHCP сервера на маршрутизаторе Mikrotik с помощью атаки DHCP starvation. Для автоматизированной атаки воспользуемся программой Yersinia:





На маршрутизаторе проверяем адреса, которые выданы из пула DHCPсервером:



Перезагрузите ПК FSLи проверьте, что ПК получил новый IP-адрес от нашего сервера.

