Правительство Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

(НИУ ВШЭ)

Московский институт электроники и математики им. А.Н. Тихонова

Лабораторная работа № 2

по дисциплине «Проектный семинар по информационной безопасности»

|  |
| --- |
| Студент гр. БИБ211  \_\_\_\_\_\_\_\_\_\_\_\_\_ А.И. Семененя  «17» декабря 2021 г. |
| Руководитель  Заведующий кафедрой информационной безопасности киберфизических систем  канд. техн. наук, доцент  \_\_\_\_\_\_\_\_\_\_\_\_\_\_О.О. Евсютин  «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2021 г. |

Москва 2021

**Цель:** получение знаний о локальных атаках MITM (man-in-the-middle), а также принципах работы протоколов ARP и DHCP.

**Вариант 1**

**Параметры:**

Сеть NAT 192.168.10.0/27

Gateway 192.168.10.10

DNS 192.168.10.10

DHCP – работает

**Атакующая машина (X):**

**IP-адрес:** 192.168.10.16/27

**MAC-адрес:** fe80::cf51::3130::cff0::797d/64

**Атакуемая машина (N):**

**IP-адрес:** 192.168.10.17/27

**MAC-адрес:** fe80::8dec::8525::5818::59c9/64

**Ход работы**

**Часть 1. DHCP-spoofing**

1. Устанавливаем на атакующую машину пакеты wireshark и ettercap.
2. Запускаем wireshark через терминал, в нём запускаем логирование пакетов на сетевом адаптере.
3. Применяем фильтр DHCP-пакетов:



Рисунок 1

1. С помощью команд *sudo dhclient –r*, *sudo dhclient* сбрасываем настройки сетевых адаптеров на атакуемой машине.
2. В Wireshark на атакующей машине видим перехваченные пакеты.

Изображение выглядит как текст, стол

Автоматически созданное описание

Рисунок 2

1. Фильтруем полученные пакеты по протоколу, оставляя только DHCP-пакеты.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 4

1. Запускаем Ettercap на атакующей машине, выбираем “Sniff” -> “Unified sniffing”. В меню “MITM” выбираем пункт “DHCP spoofing” и вводим настройки ложного DHCP-сервера.
2. Вновь сбрасываем DHCP-настройки атакуемой машины. Новые настройки таковы: Изображение выглядит как текст

   Автоматически созданное описание

Рисунок 5

1. Ettercap показывает нам, что злоумышленник «отработал».



Рисунок 6

1. Анализируем полученные пакеты в Wireshark:

Изображение выглядит как стол

Автоматически созданное описание

Рисунок 7

Атака не была успешной, в чём можно убедиться, проверив доступ к интернету на атакуемой машине утилитой ping.

1. Перезагрузим машины для перехода к следующей части работы.

**Часть 2. ARP-spoofing**

**Машина 1 (атакующая):**

**IP-адрес:** 192.168.10.16/27

**MAC-адрес:** fe80::cf51::3130::cff0::797d/64

**Машина 2:**

**IP-адрес:** 192.168.10.17/27

**MAC-адрес:** fe80::8dec::8525::5818::59c9/64

**Машина 3:**

**IP-адрес:** 192.168.10.19/27

**MAC-адрес:** fe80::f2e2::bade::508f::e6e6/64

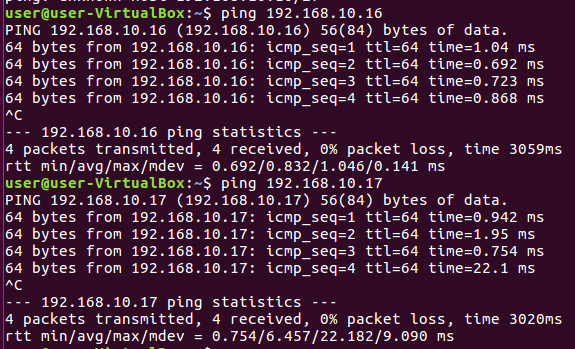
1. Добавляем третью виртуальную машину.
2. Убеждаемся, что все три машины доступны друг для друга: 

Рисунок 8

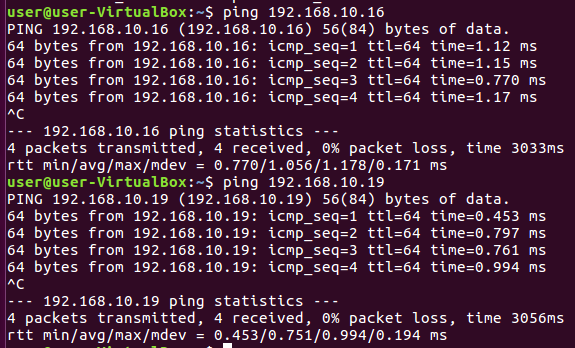


Рисунок 9

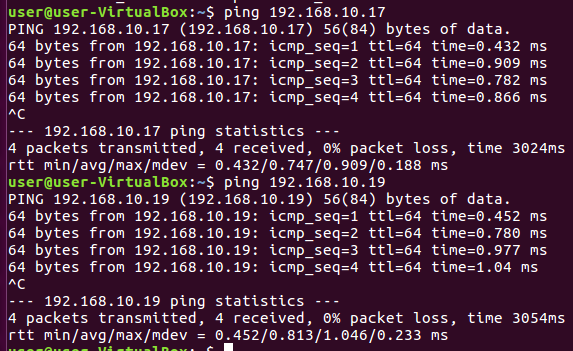


Рисунок 10

1. Фиксируем состояние ARP-таблиц каждой из машин.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 11

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 12

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 13

1. На атакующей машине запускаем Ettercap и Wireshark в новом терминале.
2. В Wireshark запускаем логирование сетевых пакетов на сетевом адаптере, сразу применяем фильтр *arp or icmp*.
3. В Ettercap переходим в режим сниффинга (“Unified sniffing”) и проводим сканирование сети (“Scan for hosts”).
4. Добавляем две цели.



Рисунок 14

1. Запускаем процесс ARP-атаки.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 15

1. Фиксируем состояние ARP-таблиц всех машин:

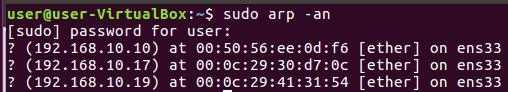


Рисунок 16

На атакующей машине (192.168.10.16) ARP-таблица не изменилась.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 17

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 18

Однако мы можем заметить, что двум другим машинам был присвоен MAC-адрес атакующей машины.

1. Анализируем пакеты, захваченные Wireshark:

Изображение выглядит как стол

Автоматически созданное описание

Рисунок 19

Мы можем заметить, что в качестве цели атакующая машина использует все IP из диапазона.

1. Останавливаем процесс атаки в Ettercap.
2. Фиксируем состояние ARP-таблиц всех машин:

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 20

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 21

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 22

Мы можем заметить, что машины снова вернулись к тем MAC-адресам, которые они использовали до атаки.

**Выводы по выполненной работе**: мы закрепили принципы работы протоколов ARP и DHCP, получили знания о локальных атаках MITM, а также протестировали работу пакета ettercap.