Сабирзянова А.М.

11-901

ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТИ НЕПРАВИЛЬНО СКОНФИГУРИРОВАННОЙ NFS SHARE. ФОРЕНЗИКА.

Содержание:

[**1) Развернуть виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения предыдущих лабораторных работ.**](#_uu8z8epeq61h) **1**

[1.1 Открываем машины](#_8crr07qz1gun) 2

[**2) Убедиться в корректной настройке сети между Metasploitable и Kali Linux**](#_w7pebhsi1c35) **2**

[2.1 Узнаем и пингуем IP адреса друг друга](#_k9lz8wscxpqy) 2

[**3) Атака на Metasploitable**](#_4ph5puudv7ov) **2**

[3.1 Сканируем Metasploitable с помощью команды nmap /var/tmp/scan.txt](#_tbitx2bcsjq1) 3

[3.2 Определяем порты сервисов rpcinfo, nfs и ssh, и их статусы](#_r00jlmeoy4h6) 3

[3.3 Оцениваем работы NFS сервера](#_2rz54tw4aw7n) 3

[**4) Использование неправильно сконфигурированной NFS Mount.**](#_tg9qlc80lyd9) **4**

[4.1 Создание пары ключей SSH и сохранение их в файле key\_file](#_l6074gcam9br) 5

[4.2 Монтируем файловую систему Metasploitable.](#_qmajkak67qjm) 5

[4.3 Изменяем файл authorized\_keys машины-жертвы.](#_t5bvmkm7abl1) 6

[4.4 Получаем root права](#_ywioznwi11fi) 6

[**5) Форензика**](#_adhf95qhzggn) **6**

[**6) Оформление результатов работы**](#_bb4tf6unt5c4) **7**

## 

## 1) Развернуть виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения предыдущих лабораторных работ.

Цель: Развернуть машины для работы

Начальная ситуация: Машины остановлены

Алгоритм:

### 1.1 Открываем машины

Конечное состояние: машины развернуты

## 2) Убедиться в корректной настройке сети между Metasploitable и Kali Linux

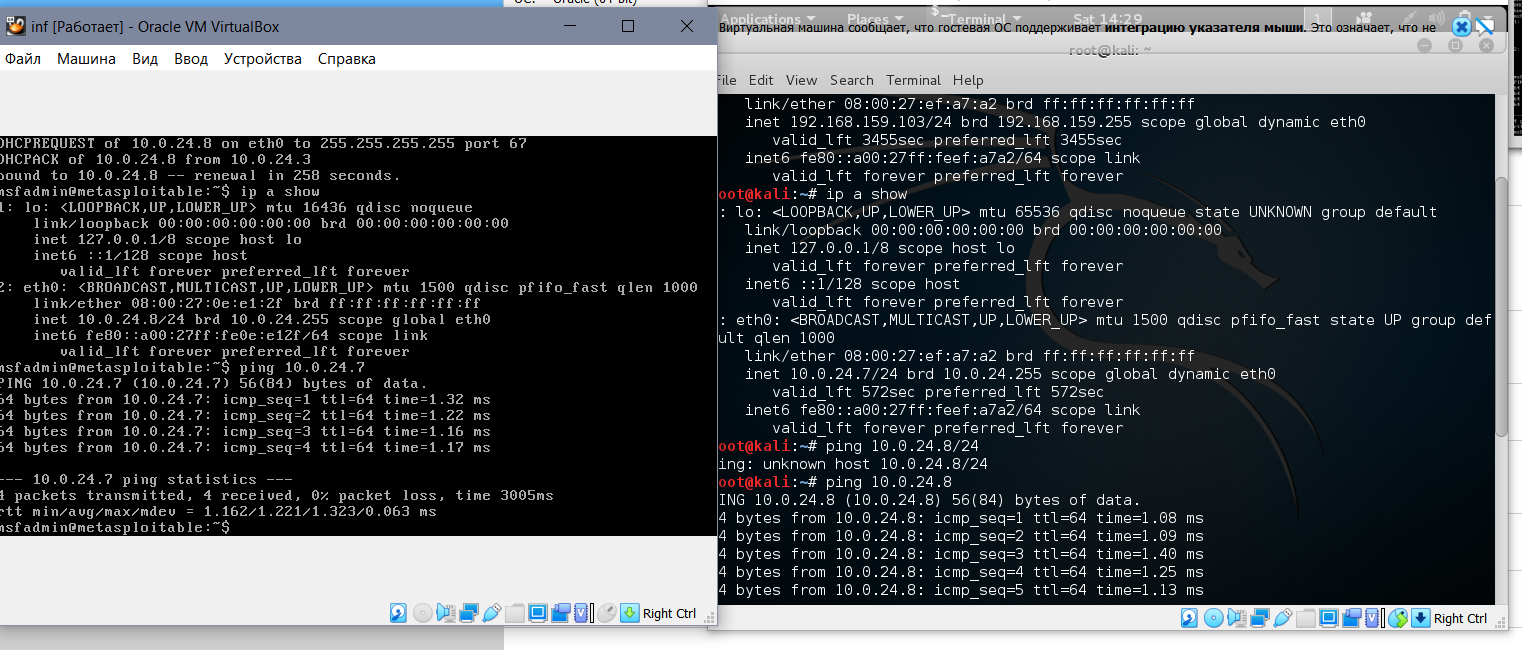
Цель: Убедиться что сеть настроена

Начальная ситуация: Неизвестность

Алгоритм:

### 2.1 Узнаем и пингуем IP адреса друг друга

KL\_IP = 10.0.24.7

MS\_IP = 10.0.24.8

Конечное состояние: получены ip адреса, убеждаемся, что связь есть

## 3) Атака на Metasploitable

Цель: обнаружить слабые места машины Metasploitable

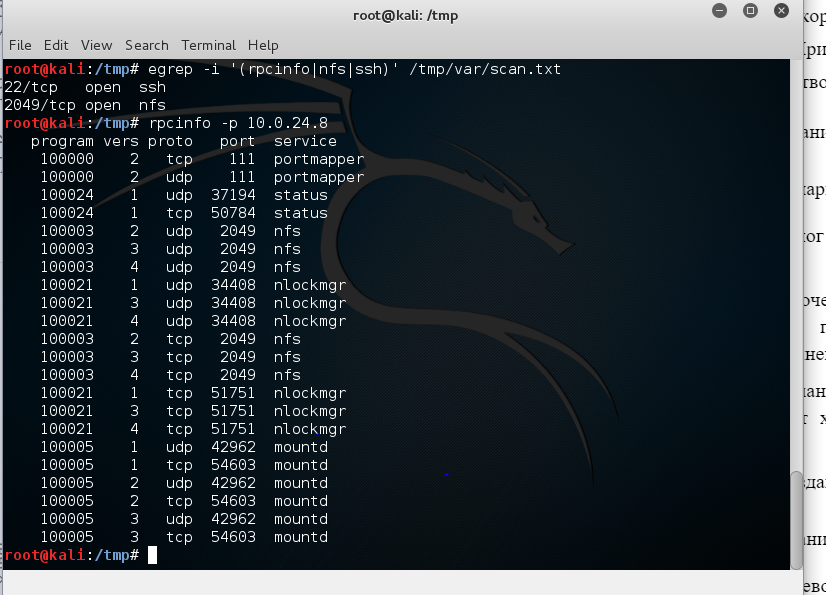
Начальная ситуация: уезвимостей не обнаружено

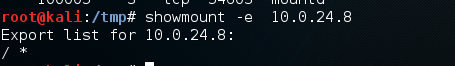
Алгоритм:

### 3.1 Сканируем Metasploitable с помощью команды nmap /var/tmp/scan.txt

### 3.2 Определяем порты сервисов rpcinfo, nfs и ssh, и их статусы

### 3.3 Оцениваем работы NFS сервера





Конечное состояние: уязвимость найдена

## 4) Использование неправильно сконфигурированной NFS Mount.

Цель: получить доступ к Metasploitable

Начальная ситуация: доступа нет

Алгоритм:

### 4.1 Создание пары ключей SSH и сохранение их в файле key\_file

### 4.2 Монтируем файловую систему Metasploitable.

### 4.3 Изменяем файл authorized\_keys машины-жертвы.

### 4.4 Получаем root права

Конечная цель: доступ к Metasploitable получен.

## 5) Форензика

Цель: Выявить атаку

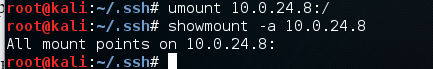
Начальное состояние: атака не выявлена

Алгоритм:

5.5 Просмотрим список подключенных машин к серверу NFS



5.6 Размонтируем файловую систему машины-жертвы, убедимся в её отсутствии командой df –k, командой showmount –a убедимся, что ip адрес атакующей машины исчез.



Конечное состояние: атака выявлена и отбита

## 6) Оформление результатов работы

