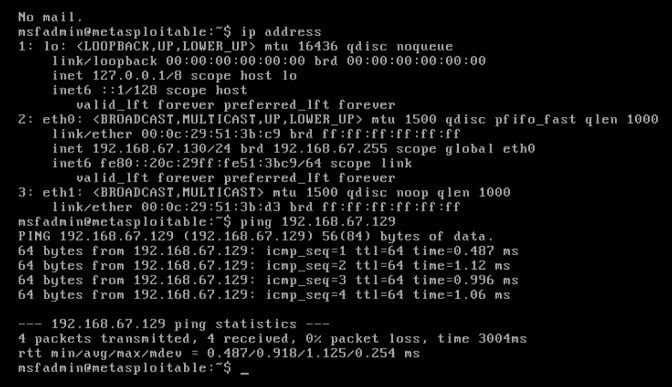
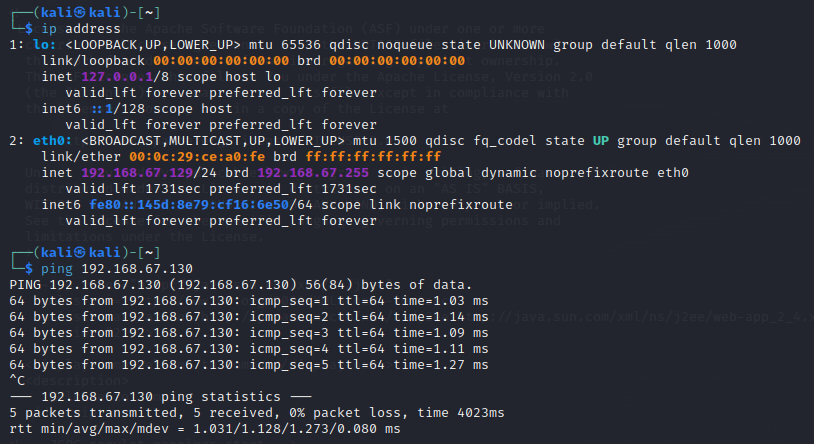
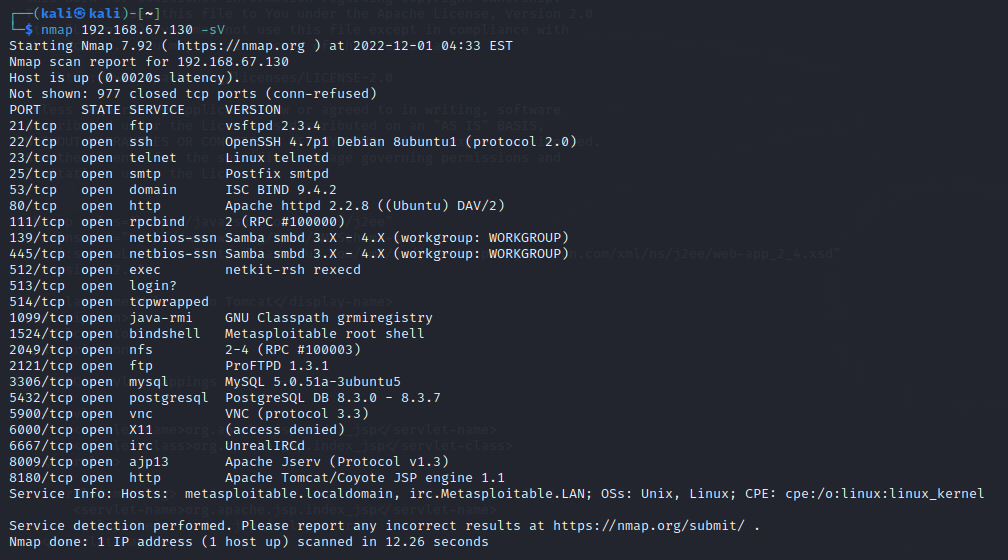
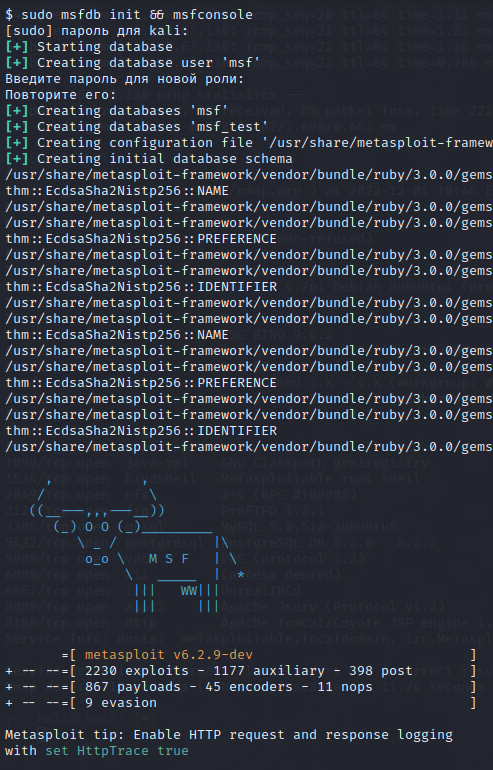
# Подготовка

1. Проверка пинга
2. Сканируем состояние портов на машине



1. Заходим в msfconsole

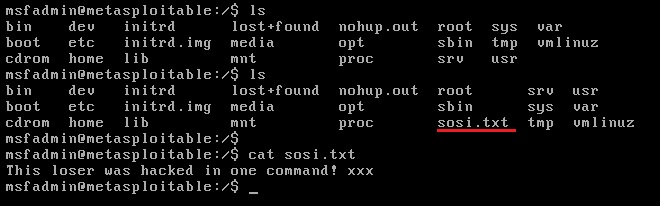


# Уязвимость 1: bindshell 1524

Подключаем терминал к целевому серверу



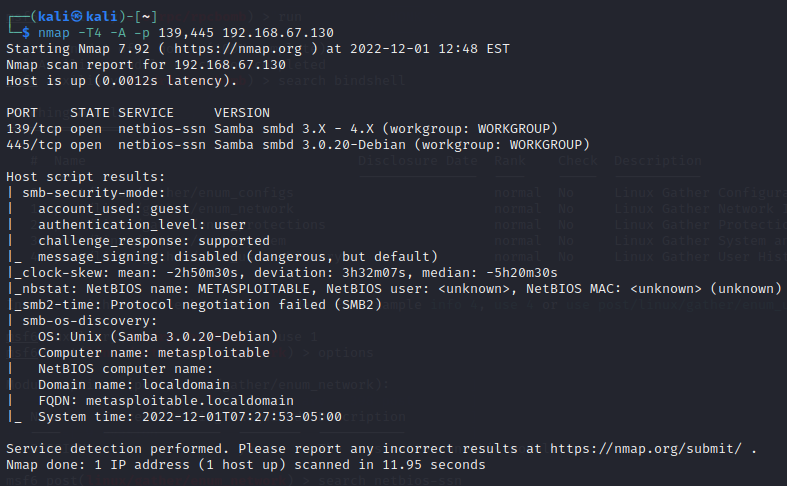


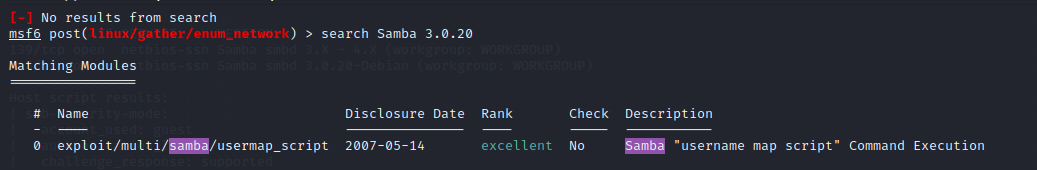


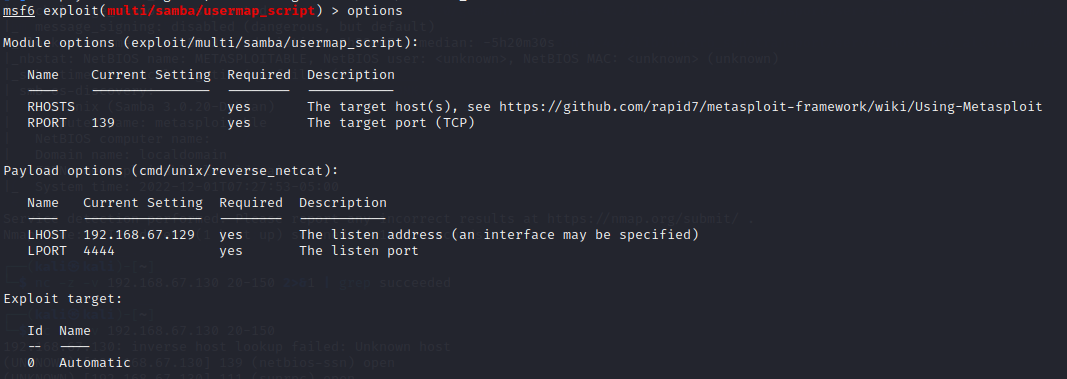
Bindshell — это обычная оболочка, такая же, как командная строка терминала Linux или командная строка (cmd) в Windows, но нужен IP-адрес сервера и инструмент netcat. Netcat (или nc) — это утилита командной строки, которая читает и записывает данные через сетевые подключения, используя протоколы TCP или UDP. Модуль Linux ядра netconsole позволяет экспортировать консоль на другую машину по сети.

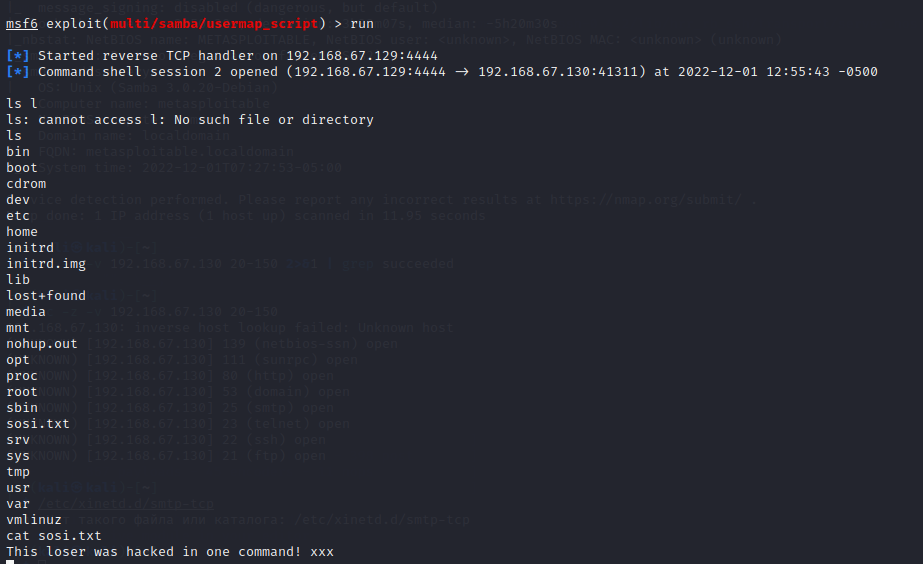
\*Чтобы использовать эту утилиту в таком ключе, она должна быть установлена на обе машины (атакующую и жертву)

# Уязвимость 2: netbios-ssn 139









NetBIOS - cетевая базовая система ввода-вывода. Это программный протокол, который позволяет приложениям, ПК и настольным компьютерам в локальной сети (LAN) взаимодействовать с сетевым оборудованием и передавать данные по сети. Все виды информации, такие как ваш домен, имена рабочих групп и систем, а также информация об учетной записи могут быть получены через NetBIOS.

Список ресурсов, список активных сессий и многое другое, доступное через нулевую сессию: доступ по нулевой сессии представляет собой возможность неавторизованного подключения к хосту с операционной системой, основанной на Windows NT (или ОС семейства UNIX с установленным пакетом Samba) с пустым логином и паролем.