### **Proof of Concept (PoC) Report**

### **Task 2: Securing SSH Access & Mitigating Brute-Force Attacks**

### **1. Overview**

### This Proof of Concept (PoC) highlights security vulnerabilities arising from improperly configured SSH settings, including root access and password-based authentication. The objective is to demonstrate the risks of such configurations through a brute-force attack and implement security enhancements to mitigate them.

### **2. Key Steps**

### **Configuration:**

### Enable SSH and configure it to permit root login and password authentication. **Exploitation:**

### Execute a brute-force attack using tools like Hydra to exploit weak SSH settings. **Mitigation:**

### Restrict root login, enforce key-based authentication, and implement fail2ban to prevent brute-force attacks.

### **3. Environment Setup**

#### **3.1 Activating SSH**

### SSH was activated and set to initiate at system startup with the following commands:

### 

### 

#### **3.2 Enabling Root Login & Password-Based Authentication**

### The SSH settings in were modified to permit root login and authentication via passwords. **Configuration Modifications:**

### 

### 

### **4. Exploitation Phase**

#### **4.1 Conducting a Brute-Force Attack**

### A brute-force attack was executed using Hydra to exploit the weak authentication setup **Command Used:**

### 

### 

### **5. Security Enhancements**

#### **5.1 Restricting Root Login & Password Authentication**

### The SSH configuration was adjusted to disable root login and enforce key-based authentication. **Configuration Changes:**

### 

### 

#### **5.2 Enabling Key-Based Authentication**

### SSH key-based authentication was set up by generating a key pair and adding the public key to the authorized keys file. **Commands Used:**

### 

### 

#### **5.3 Validation of Security Measures**

### Attempts to log in as root or use password authentication were blocked following the implementation of security measures. **Verification Command:**

### 

### 

### **6. Summary**

### This PoC effectively demonstrated how weak SSH configurations can be exploited and the importance of hardening SSH settings. By disabling root login, enforcing key-based authentication, and deploying measures against brute-force attacks, the security posture of SSH was significantly improved.

### .

### 