## **Phase 3: Defensive Strategy Proposal (what should we do )**

### 1. Objective

The goal of Phase 3 is to implement a defensive mechanism that protects the victim machine (Metasploitable3) from the same SSH brute-force attack that was executed in Phase 1. After applying the defense, the attack is repeated to verify that the system is now secure.

### 2. Defense Mechanism

To mitigate the SSH brute-force vulnerability, we should implement the following defensive measures on the victim machine:

* **Disabled SSH Service**: The SSH service (ssh) should stopp and disabled to prevent external access.
* **Installed Fail2Ban**: A log-based intrusion prevention tool (fail2ban) was installed and configured to block IPs after multiple failed login attempts.
* **User Access Restriction**: The vagrant account was disabled, and a strong-password policy was enforced on newly created accounts.

Commands that will use:

sudo systemctl stop ssh

sudo systemctl disable ssh

sudo apt-get install fail2ban

sudo usermod -L vagrant

### 3. Testing & Validation

To validate the effectiveness of the defense, we should attempt the same SSH brute-force attack using Metasploit with the same configuration used in Phase 1.

* **Result**: The attack should be failed. Because the SSH port was closed and no connection could be established, demonstrating that the defense was successful.
* **Fail2Ban Status**: Logs shoud confirm that after multiple failed attempts (when SSH was temporarily enabled), the attacking IP was banned.

### 4. Before-and-After Comparison

|  |  |  |
| --- | --- | --- |
| **Metric** | **Before Defense** | **After Defense** |
| SSH Service | Enabled | Disabled |
| Brute-force Success | Shell access achieved | Connection refused |
| Credentials Access | vagrant:vagrant used | Account disabled |
| Logs | No protection or detection | Fail2Ban banned attacker IP |
|  |  |  |

### 5. Evidence

* Screenshot 1: Showing SSH service disabled or systemctl status ssh.
* Screenshot 2: Fail2Ban installation and configuration (/etc/fail2ban/jail.conf or similar).
* Screenshot 3: Logs showing attacker IP banned.
* Screenshot 4: Failed brute-force attempt from Metasploit after defense.