**King Fahad University of Petroleum and Minerals**

**ICS344 Project Report**

**Group number: 06**

**Section: F08**

**Phase3**


| Duaa Alhassan | Zainab Almaskeen. | Renad Alqahtani |
|---|---|---|
| 202168790 | 202175370 | 202169930 |


**3/5/2025**

## Phase 3: Defensive Strategy Proposal

The primary goal of Phase 3 is to implement a defense mechanism to protect the victim machine (Metasploitable3) from the attack performed in Phase 1, and to demonstrate the effectiveness of this defense. In this case, Fail2Ban is used to defend against brute-force SSH attacks.

### 1- Defense Mechanism Selection:

- The chosen defense mechanism is Fail2Ban, an intrusion prevention tool.
- Fail2Ban's function is to monitor log files for malicious behavior (e.g., repeated failed login attempts) and automatically ban the offending IP addresses.
- The specific goal is to mitigate brute-force SSH attacks.

### 2- Fail2Ban Installation and Configuration (Victim Machine):

Fail2Ban is installed on the Metasploitable3 victim machine and it is configured to monitor SSH login attempts.

```
vagrant@metasploitable3-ub1404:~$ sudo apt-get install -y fail2ban iptables
Reading package lists... Done
Building dependency tree
Reading state information... Done
iptables is already the newest version.
```

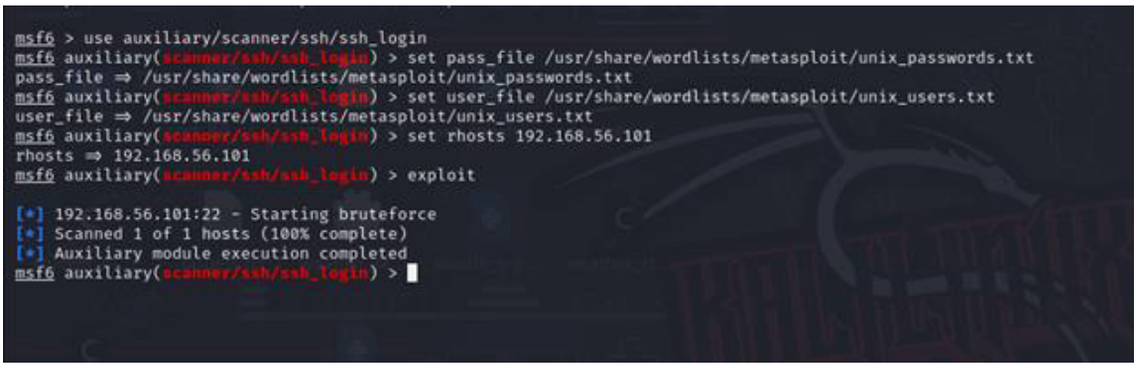
### 3- Before-Attack Verification:

- The SSH "jail" in Fail2Ban is checked to ensure it's active and ready.
- The output shows: "Currently failed: 0 and Currently banned: 0".
- This indicates that Fail2Ban is running and no previous attack activity has been detected.

```
vagrant@metasploitable3-ub1404:~$ sudo fail2ban-client status ssh
Status for the jail: ssh
|- filter
|  |- File list:        /var/log/auth.log
|  |- Currently failed: 0
|  `- Total failed:     0
`- action
   |- Currently banned: 0
   |  `- IP list:
   `- Total banned:     0
vagrant@metasploitable3-ub1404:~$
```

### 4- Attack Execution (Attacker Machine - Kali VM):

- The same attack from Phase 1 is re-executed from the Kali VM.
- The attack targets SSH port 22 on the victim machine.
- The text notes that the attack execution might not show immediate output, indicating Fail2Ban's active blocking.



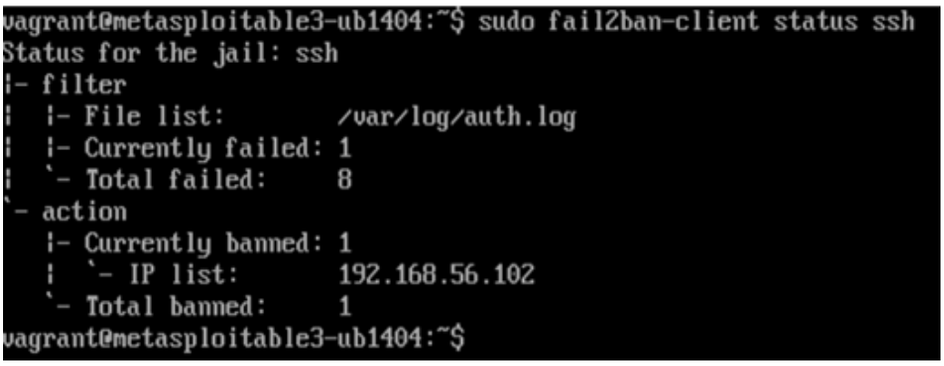

## 5- Fail2Ban Result (Victim Machine):

Fail2Ban successfully detects and blocks the brute-force attack.

The output shows:

- "Currently banned: 1"
- "Total failed attempts: 8"

This confirms that Fail2Ban has automatically banned the attacker's IP after 8 failed login attempts.




The results are compared to the successful attack in Phase 1, and it is concluded that Fail2Ban effectively thwarted the attack, demonstrating the improvement in security.