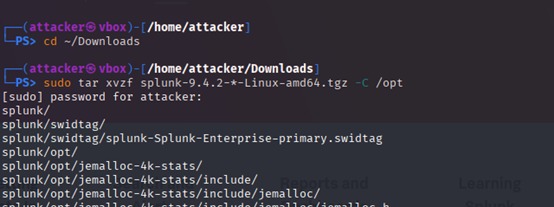
**Phase 2**

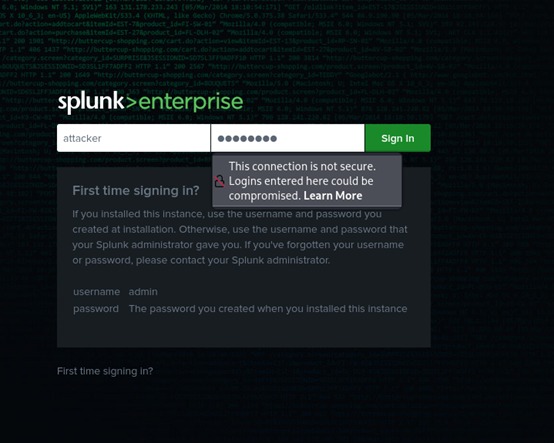
**1. Objective**

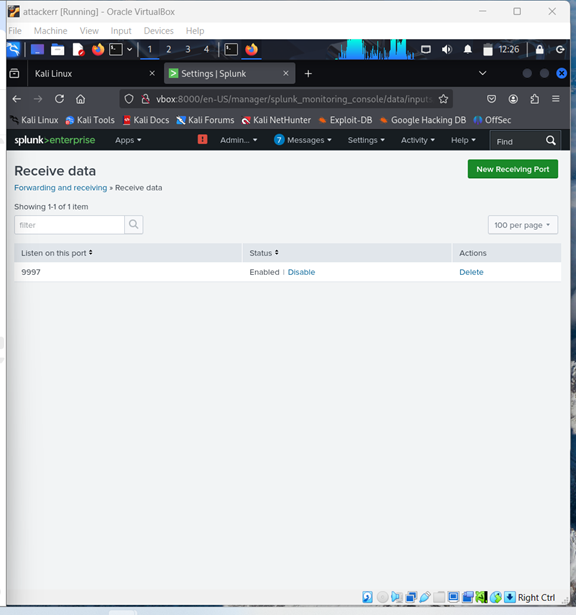
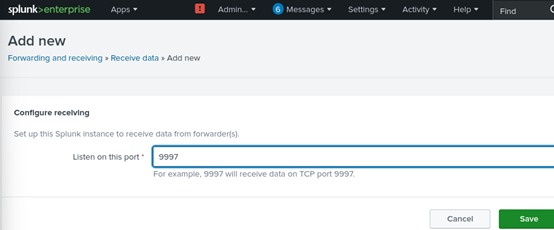
Integrate logs from both the victim (Metasploitable3) and attacker (Kali) into a SIEM and visualize attack activity.

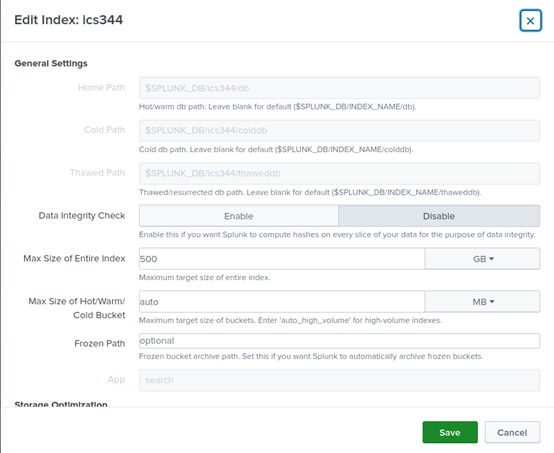
**2. Environment**

* **SIEM Server (Kali)**
  + Splunk Enterprise 9.x running at https://localhost:8000
  + Admin user: attacker / asdfasdf

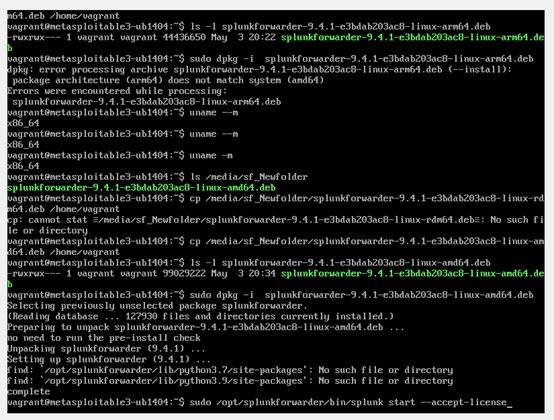
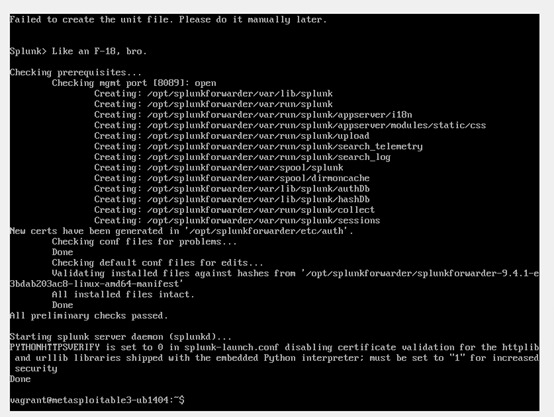




* + Receiving port: **9997**
  + 
* Edit index:



* **Victim (Metasploitable3)**
  + Ubuntu 14.04 VM
  + Target SSH service at 192.168.56.101
  + Splunk forwarder installation using sharefolder in metasploit3:



**3. Log Forwarding Status**

* **The victim’s logs were already collected, compressed, and sent to the attacker. Then, they were uploaded to Splunk.**