**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**
* **Victim (Metasploitable3)**
  + Ubuntu 14.04 VM
  + Target SSH service at 192.168.56.101
  + Attempts made to install Splunk UF (versions 9.3.2, 9.4.1, 9.4.2) and Wazuh Agent

**3. Steps & Attempts**

**3.1 Splunk Forwarder Installation**

* Tried .deb packages for Splunk UF v9.4.2, 9.4.1, 9.3.2 on the victim → **dpkg** errors (“not a Debian format archive”) because the VM had no Internet/DNS and the wrong architecture link was sometimes fetched.
* Adjusted VirtualBox networking (NAT ↔ Host-only on Adapters 1 & 2) to give the victim Internet access.
* Re-downloaded using the browser’s “Copy wget link” for the 64-bit .deb, but still encountered installation failures.

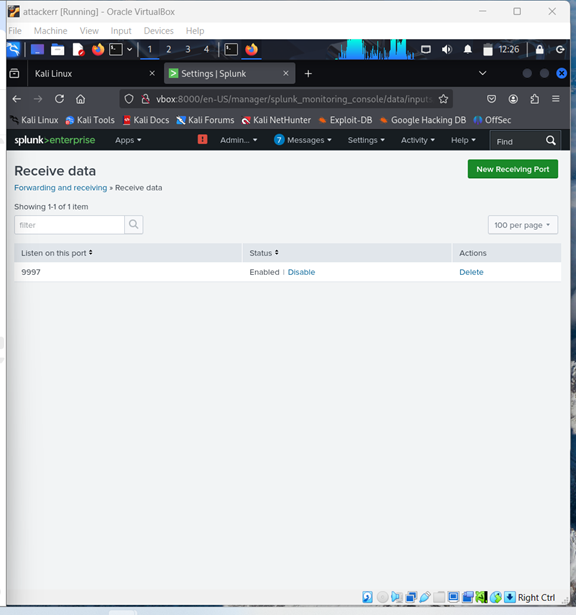
**3.2 Wazuh Agent Installation**

* Switched to Wazuh Agent as an alternative: fetched wazuh-agent\_4.7.2-1\_amd64.deb → same “not a Debian format archive” error due to the victim’s network/DNS issues.
* Confirmed wget was pulling small HTML error pages, not the real packages.

**4. Final SIEM Server Configuration**

* **Splunk Enterprise** on Kali:
  + Receiving port 9997 enabled ✓
  + ics344 index created ✓
  + Splunk Web accessible at https://localhost:8000 (user: attacker / asdfasdf) ✓

**Screenshot 1**: Splunk “Receive data” page showing port 9997 enabled.



**5. Log Forwarding Status**

Despite multiple attempts over two days, no agent on the victim could successfully install and register with Splunk or Wazuh.

**Screenshot 2**: Victim directory listing showing the downloaded .deb files and the dpkg error.  
A computer screen shot of a computer program

AI-generated content may be incorrect.