Troubleshooting Guide for SOC Simulator Home Lab

**1. General Troubleshooting Steps**

* **Verify Physical & Virtual Connectivity**
  + Confirm that all VMs are powered on.
  + Check network adapter settings in VMware (ensure correct VMnet is assigned).
  + Ping between VMs to verify connectivity (e.g., from Kali Linux to the Domain Controller).
* **Review Logs**
  + Check system logs on to each VM for error messages.
  + Use built-in Windows Event Viewer on Windows machines and journalctl or /var/log files on Linux systems.
* **Double-Check Configuration Files**
  + Confirm that IP addresses, subnet masks, and gateways are correctly set with your placeholder values.
  + Verify that DNS settings point to the appropriate server (typically your Domain Controller).

**2. Domain Controller & Windows Server Issues**

**Issue: Domain Controller Not Promoting or Starting AD DS**

* **Check Installation Logs:**
  + On Windows Server, review the setup logs in the Event Viewer.
  + Look for errors related to AD DS installation or promotion.
* **Fixes:**
  + **Re-run the Promotion:** If the promotion process fails, rerun the command:

PowerShell

Install-ADDSForest -DomainName "evilcorp.local"

* + **Network Configuration:** Ensure the static IP (e.g., 10.0.100.10) is set correctly and that there’s no IP conflict on the network.
  + **DNS Settings:** The Domain Controller should use its own IP as the primary DNS server.

**Issue: Windows Logging Policies Not Forwarding Logs**

* **Check Audit Policy Settings:**
  + Confirm that the audit policies have been enabled properly using AuditPol.
  + Run AuditPol /get /category:\* to verify current settings.
* **Fixes:**
  + Re-run the audit commands to ensure success.
  + Restart the Windows Event Log service if changes are not reflected.

**3. Wazuh Server & Agent Troubleshooting**

**Issue: Wazuh Agent Failing to Connect to the Wazuh Server**

* **Symptoms:**
  + Agent logs do not show registration.
  + Wazuh server shows no incoming agents.
* **Troubleshooting Steps:**
  + **Verify Agent Configuration:**
    - Open ossec.conf on the agent (Windows or Linux) and ensure the <address> tag contains the correct <Wazuh\_Server\_IP>.
  + **Network Connectivity:**
    - Ensure the agent can ping <Wazuh\_Server\_IP>.
  + **Service Status:**
    - At the agent, restart the service with:

PowerShell

net stop wazuh-agent && net start wazuh-agent

* + **Agent Registration:**
    - On the server, run:

bash

/var/ossec/bin/agent-auth -m <Wazuh\_Server\_IP>

* + - Check for successful agent registration in /var/ossec/logs/ossec.log.

**Issue: Wazuh Server or API Not Starting**

* **Troubleshooting Steps:**
  + **Service Check:**
    - On the Wazuh VM, check status using:

bash

sudo systemctl status wazuh-manager

* + **Dependency Issues:**
    - Reinstall any missing dependencies using:

bash

sudo apt install curl apt-transport-https lsb-release gnupg -y

* + **Log Inspection:**
    - Review /var/ossec/logs/ossec.log for startup errors.

**4. Security Onion Troubleshooting**

**Issue: Security Onion Web Interface Unreachable**

* **Troubleshooting Steps:**
  + **Network Interface Configuration:**
    - Ensure the network interface is correctly configured in /etc/network/interfaces with your <Security\_Onion\_IP> and proper gateway settings.
    - Verify by running:

bash

sudo netplan apply

* + **Service Check:**
    - Restart Security Onion services if needed.
    - Check for errors in /var/log/ related to Security Onion.
  + **Access URL:**
    - Double-check that you are using https://<Security\_Onion\_IP>/ in your browser.
    - Ensure any firewall rules (either on the host or VM) are not blocking access.

**Issue: No Alerts or Logs in Kibana Dashboard**

* **Troubleshooting Steps:**
  + **Data Ingestion:**
    - Ensure agents (Wazuh or Syslog) are sending data correctly.
  + **Dashboard Configuration:**
    - Refresh the dashboard and confirm that the time filter is set correctly.
  + **Log Check:**
    - Check the log files on the Security Onion VM for any ingestion errors.

**5. Attack Simulation & Monitoring Issues**

**Issue: Attack Simulations Not Being Detected**

* **Troubleshooting Steps:**
  + **Verify Logging:**
    - Ensure that your Windows logging policies are enabled (audit policies, PowerShell logging, etc.).
  + **Network Traffic Monitoring:**
    - Confirm that Security Onion is correctly monitoring the interface connected to your simulated attacks.
  + **Check Wazuh Alerts:**
    - On the Wazuh Dashboard, review alert rules and verify that the simulation activity matches detection rules.
  + **Simulated Attack Tools:**
    - Re-run a simulation from Kali Linux (e.g., password spraying) and monitor logs on both the Domain Controller and Wazuh Server.

**6. Additional Troubleshooting Tips**

* **Update Everything:**
  + Ensure your OS, VMs, and installed software (Wazuh, Security Onion) are fully updated to the latest stable releases.
* **Clear Cache & Restart Services:**
  + Sometimes restarting a service or even the VM can resolve transient issues. Don’t hesitate to reboot.
* **Official Consult Documentation:**
  + Use the Wazuh Documentation and Security Onion Documentation for detailed troubleshooting guides and community support.
* **Document Your Fixes:**
  + Keep a log of any issues and the steps you took to resolve them. This can be invaluable for future troubleshooting or for sharing with peers.

By following these steps, you should be able to identify and fix the most common issues within your lab. Remember, a little troubleshooting can go a long way—if all else fails, rebooting is the IT equivalent of “turning it off and on again.” Happy hunting!