Splunk & Sysmon

Splunk is a SIEM (Security Information & Event Management) tool that allows you to have a central platform where you can receive inputs for multiple log data sources, for monitoring purposes

- Log - an event that contains fields that contains specifications of the event
- Ex: Grocery shopping log would be time of entry, what you bought, when you left, store name, type of payment, etc.
- It is easy to keep track and manage logs from one or two devices but with thousands on a network it is impossible which is what Splunk is built for!

Sysmon (System Monitor) - is a free windows system service and driver that logs detailed information about system activity into windows event log.

- Often used in cybersecurity monitoring, threat hunting, and incident response because it gives more visibility than standard windows logs.
- Features:
  - Process creation (what program ran, who, when, with which command line arguments)
  - Network connections (IP addresses, ports, processes that open the connection)
  - File creation time changes (useful for spotting time stomping attacks)
  - Driver and DLL loading
  - Registry changes
- Why Cyber Pros use it
  - Detects suspicious or malicious activity that default windows logs miss
  - Can show which process downloaded a file, which command launch PowerShell, etc.
  - Integrates with SIEMs like Splunk or Elastic for centralized monitoring

    - Helps in forensic investigations after an attack
- Use in Home Lab
    - Simulate a malware infection, watch it creates files, spawns processes and connects to the network (logged by Sysmon)
    - Send those logs to Splunk in another VM for analysis
    - Sysmon is not a GUI program - you control it via command line and config XML file, which defines what events it should log

Proper Installation to VMs

- In order to properly install these machines on my VM I will install it on my host machine and go through virtual box “Shared Folders” option to transfer the downloads to the VMs. I have to do this since I have changed the network type to internal network and disabled Wi-Fi access to mitigate risks.
- After installing all applications I will disconnect the share folder access to be sure the VMs running malware has no connection to the host.

Steps to allow sharing a folder from host (virtual box settings) to VM

1. **Go into virtual box**
2. **Select VM → Settings → Shared folders → Add Folder Directory** (to the right)

Next Steps (Windows 10 VM)

1. **Run the Windows VM**
    - Start it from VirtualBox Manager so you see the VM’s desktop.
2. **Open the VM’s Top Menu Bar**
    - Make sure you’re in the **VM window** (not VirtualBox Manager).

- At the top, you should see:

  Machine | View | Input | Devices | Help.

3. **Insert the Guest Additions CD Image**
   - Click **Devices → Insert Guest Additions CD Image**.
   - If prompted to download it, allow VirtualBox to do so.
4. **Install Guest Additions Inside the VM**
   - In Windows File Explorer (inside the VM), open **This PC**.
   - Double-click the **CD Drive (VirtualBox Guest Additions)**.
   - Run **VBoxWindowsAdditions.exe**.
   - Follow the install wizard → **Reboot the VM** when done.
5. **Access the Shared Folder**
   - After reboot, open File Explorer.
   - Go to:

     ```
     Network → VBOXSVR → <YourSharedFolderName>
     ```

   - Your host's shared files will be inside.

💡 **Tip:** If you want the shared folder to always be available, make sure **Auto-mount** and **Make Permanent** are checked in **Shared Folder Settings**.

If you want, I can send you the **exact location where Shared Folders appear in Windows 10** so you know where to look immediately after reboot — that's the step that usually trips people up.

- You have to allow Network connectivity to shared folders enable this but disable before adding malware
- Use the option read only so the VM cant add to the folder

Extra Notes

What Happens When You Install Splunk

1. **Splunk installs a local service** on your machine (Windows service or Linux daemon).
2. That service includes a **built-in web server** (by default on **port 8000**).
3. After installation finishes, you open your browser **inside the VM** and go to:

   ```
   arduino
   CopyEdit
   http://localhost:8000
   ```

   or

   ```
   cpp
   CopyEdit
   http://<VM's-IP>:8000
   ```

4. Splunk's full GUI loads from your machine itself — no internet needed.
5. From there, you configure:
   - Data inputs (e.g., read log files, monitor directories, receive forwarded logs)
   - Search & Reporting dashboards
   - Alerts and queries

Key Points

- **"localhost"** = the same machine Splunk is running on — so it works offline.
- You can also access it from another VM (if on the same lab network) by using the Splunk server VM's IP:

```
cpp
CopyEdit
http://192.168.x.x:8000
```

- The install process configures everything you need for a basic setup — you only need to add data sources afterward.

Disconnect Network Discovery and preparation before adding malware to mitigate risks

How to Disable Shared Folders in VirtualBox

1. **Shut down** your VM completely (don't just save the state).
2. In **VirtualBox Manager**, right-click your VM → **Settings**.
3. Go to **Shared Folders**.
4. In the list, select the shared folder(s) you added before.
5. Click the **minus (–)** icon to remove them.
6. Click **OK** to save settings.

Turn Off Network Discovery in Windows 10/11

1. **Open Control Panel**
   - Press **Windows key + R** → type `control` → press **Enter**.
2. Go to:

```
scss
CopyEdit
Network and Sharing Center
```

(If you don't see it, switch **View by:** to **Large icons** or **Small icons**.)

3. In the left sidebar, click:

```
nginx
CopyEdit
Change advanced sharing settings
```

4. Expand **All Networks** (or the network profile you're on — Public, Private, or Domain).
5. Under **Network Discovery**:
   - Select **Turn off network discovery**.
   - Also check **Turn off automatic setup of network-connected devices**.
6. Click **Save changes**.

Extra Lockdown for Malware Testing

In the VM's **VirtualBox Settings**:

- **Shared Folders** → Remove all.
- **General → Advanced**:
  - Shared Clipboard = Disabled
  - Drag & Drop = Disabled
- **Network → Adapter 1**:
  - Keep it on **Internal Network** (never NAT or Bridged for malware work).

✅ After doing this:

- The Windows VM won’t broadcast itself on the network.
- Malware inside the VM has one less way to move laterally to other machines.