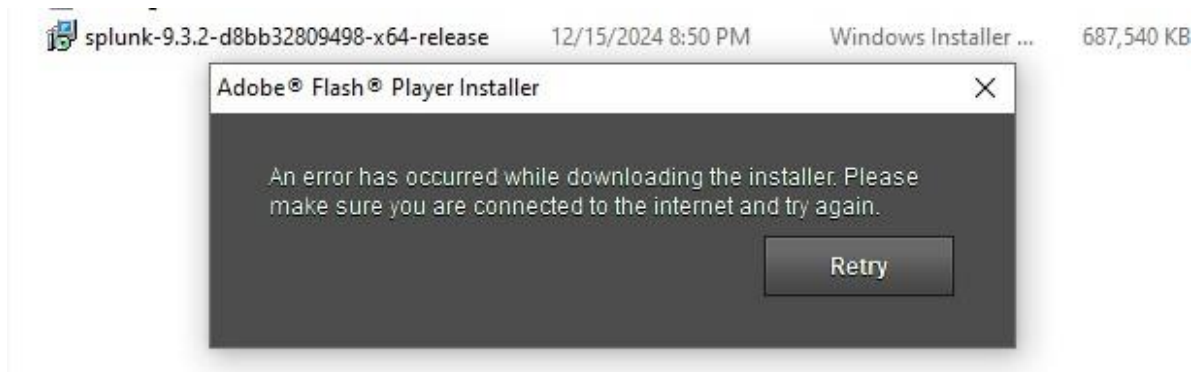
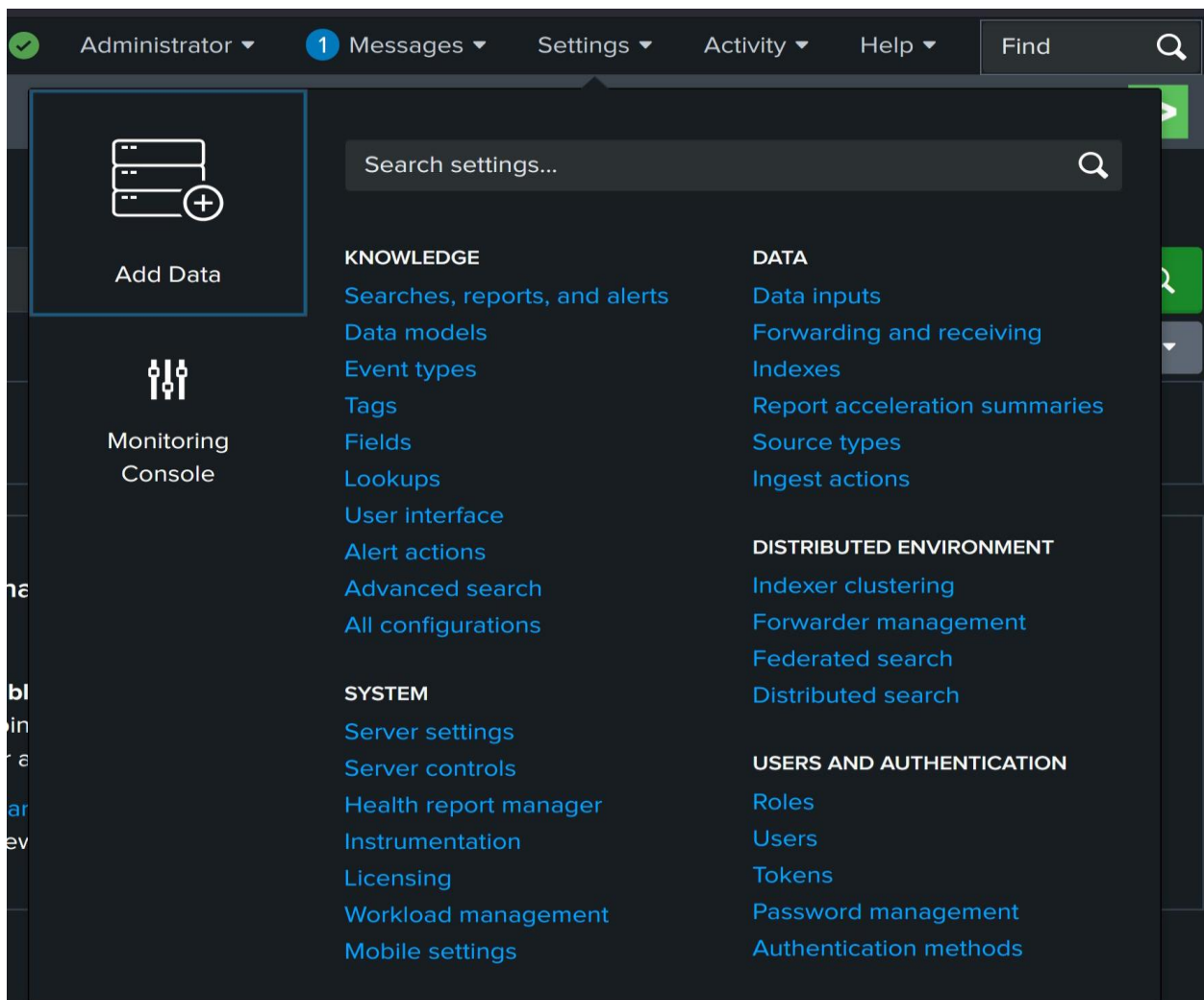


## ➤ Step 1 : Run malware :






## ➤ Step 2 : Equipped for network monitoring and recordings:

### • Screen Shot 1 :



- **Screen Shot 2 :**

Or get data in with the following methods

 <p><b>Upload</b> files from my computer</p> <p>Local log files Local structured files (e.g. CSV) <a href="#">Tutorial for adding data</a></p>	 <p><b>Monitor</b> files and ports on this Splunk platform instance</p> <p>Files - HTTP - WMI - TCP/UDP - Scripts Modular inputs for external data sources</p>	 <p><b>Forward</b> data from a Splunk forwarder</p> <p>Files - TCP/UDP - Scripts</p>
---	---	---

## Local Event Logs

Collect event logs from this machine.

- **Screen Shot 3 :**

Selected item(s)

« remove all

Application

Internet Explorer

Security

System

## • Screen Shot 4 :

>	12/20/24 8:13:58.000 PM	12/20/2024 08:13:58 PM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-GHIM6KV SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=34318 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated.
		Subject: Security ID: S-1-5-21-2511539316-984186167-484038110-1000 Account Name: ██████████ Account Domain: DESKTOP-GHIM6KV Logon ID: 0x1F9FB
		User: Security ID: S-1-5-21-2511539316-984186167-484038110-1000 Account Name: ██████████ Account Domain: DESKTOP-GHIM6KV
		Process Information: Process ID: 0xf10 Process Name: C:\Program Files\WinRAR\WinRAR.exe
		<a href="#">Collapse</a>
	Process_ID = 0xf10	host = DESKTOP-GHIM6KV   index = network   source = WinEventLog:Security   sourcetype = WinEventLog:Security