

## **Project:** Configuration and Deployment of Sysmon agent in a windows environment & visualization of its logs in Elastic SIEM.

**Overview:** Sysmon (short for System Monitor) is a Windows system service and driver from Microsoft's Sysinternals Suite. It is used for advanced system monitoring and event logging, especially for security investigations and threat detection. These logs will be viewed in the Elastic Security Information Event Management (SIEM)

### **TOOLS USED:**

- Sysmon - the zip folder is uploaded in my github
- Winlogbeat - the zip folder is uploaded in my github
- Elasticsearch zip folder - found on the ELK stack website
- Kibana zip folder - found on the ELK stack website

### **Steps:**

**Step 1:** Installation of sysmon agent, after downloading the zip file, unzip folder on your computer, run command prompt as administrator then install it, like the screenshot below;

```
C:\Users\Olunpelumi\Desktop\Sysmon>. \sysmon64.exe -i

System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2, libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

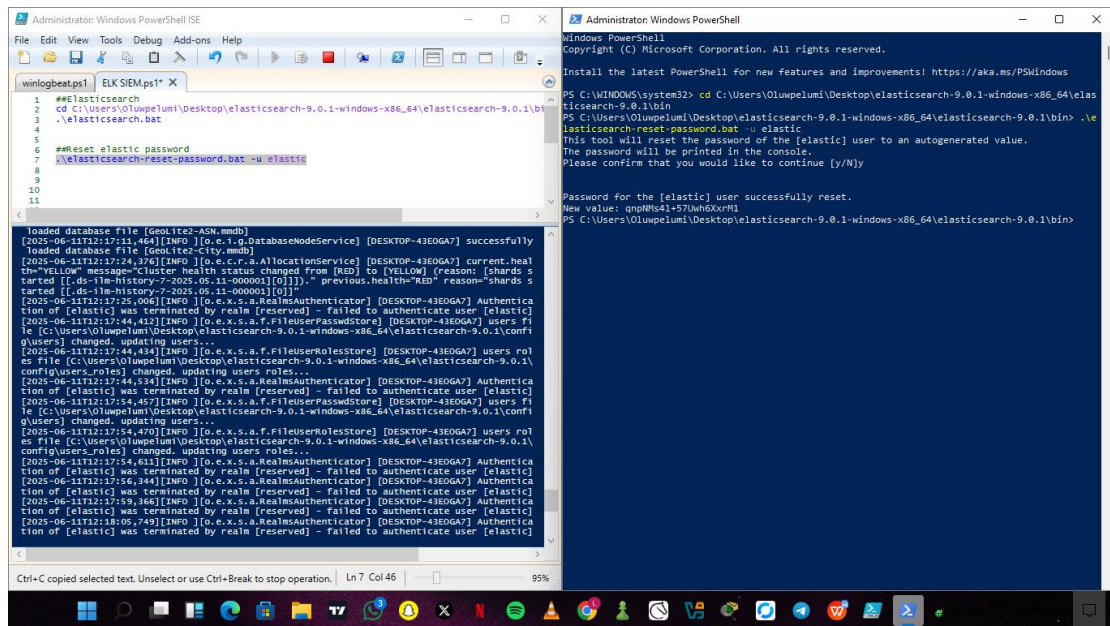
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.

C:\Users\Olunpelumi\Desktop\Sysmon>
```

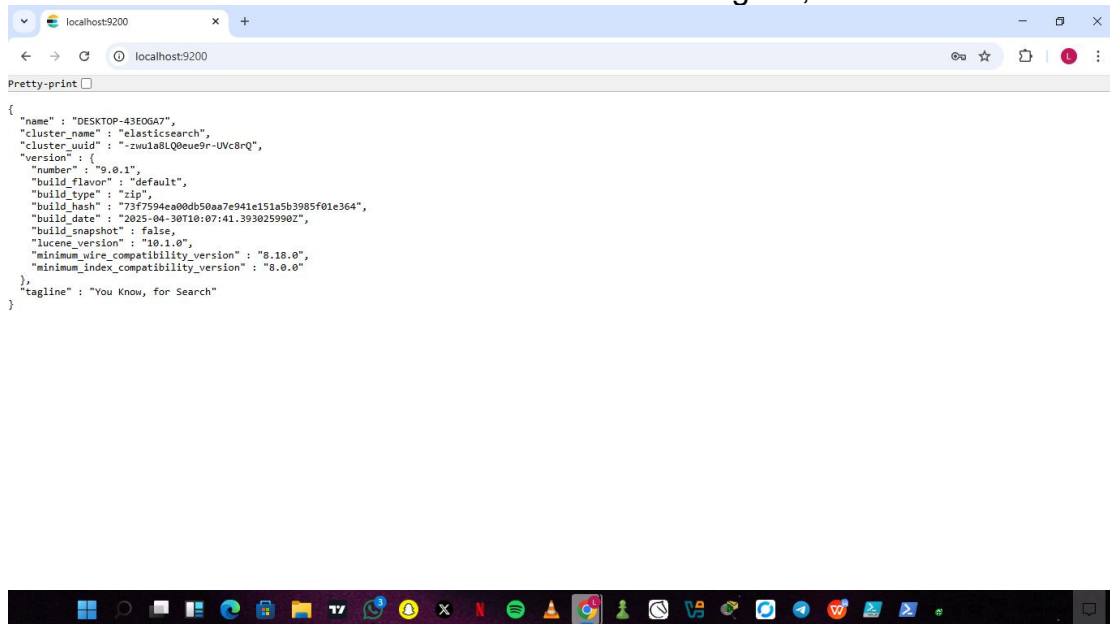
Sysmon has been installed & fully deployed.

### **Step 2:** Setup Elastic SIEM;

After Elastic & Kibana folder has been downloaded, unzip them, install elastic search first and reset password like the screenshot below



After elastic has started visit **localhost:9200** and sign in;



This shows Elastic started successfully

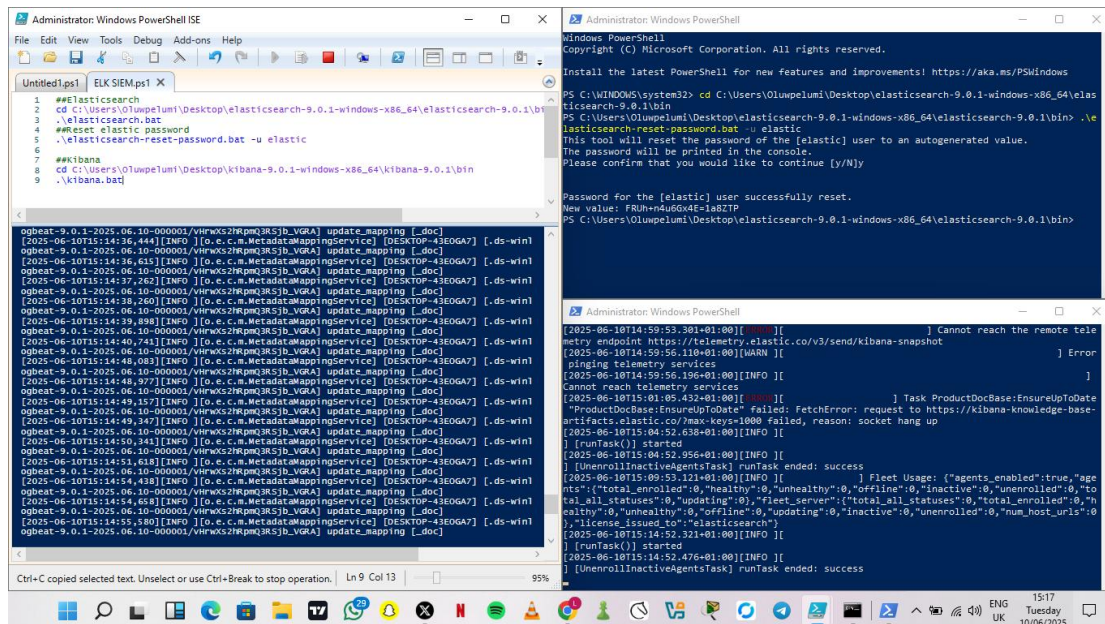
Then proceed to install kibana but before install kibana some changes has to be made in yaml file;

```
elasticsearch.hosts: ["http://localhost:9200"]
elasticsearch.username: "kibana_system"
elasticsearch.password: "the_password_you_set_for_kibana_system"
```

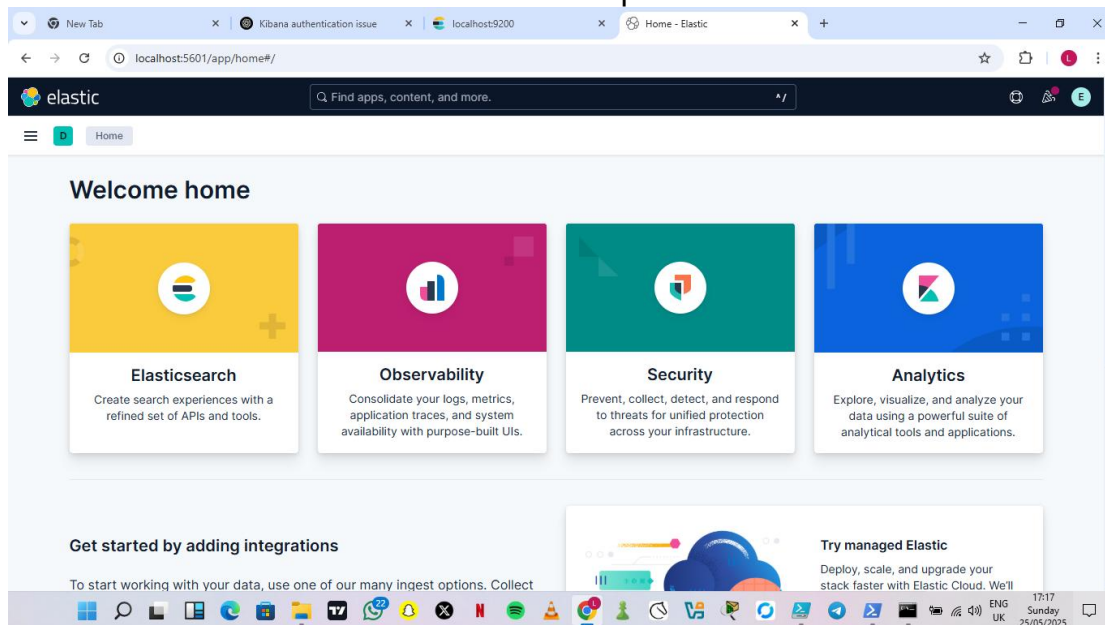
To reset kibana password use;

```
.\elasticsearch-reset-password.bat -u kibana_system
```

then save changes and install kibana when it starts proceed to your browser and visit **localhost:5601** and sign in with the elastic password.



## ELK Setup



## Elasticsearch successfully started

**Step 3:** Configure winlogbeat yaml file to integrate the sysmon logs to the elastic SIEM and install, open the yaml file and make some changes like input kibana password;

output.elasticsearch:

hosts: ["http://localhost:9200"]

username: "elastic"

password: "the elastic password"

Save & install the powershell script like the screenshot below;

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help

winlogbeat.ps1 X
1 cd C:\Users\Olupelumi\Desktop\winlogbeat-9.0.1-windows-x86_64\winlogbeat-9.0.1-windows-x86_64
2
3 Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
4
5 .\install-service-winlogbeat
6
7 Start-Service winlogbeat

PS C:\WINDOWS\system32> cd C:\Users\Olupelumi\Desktop\winlogbeat-9.0.1-windows-x86_64\winlogbeat-9.0.1-windows-x86_64
PS C:\Users\Olupelumi\Desktop\winlogbeat-9.0.1-windows-x86_64\winlogbeat-9.0.1-windows-x86_64> Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
PS C:\Users\Olupelumi\Desktop\winlogbeat-9.0.1-windows-x86_64\winlogbeat-9.0.1-windows-x86_64> .\install-service-winlogbeat
[SC] DeleteService SUCCESS

Status Name Display Name
-----
Stopped winlogbeat

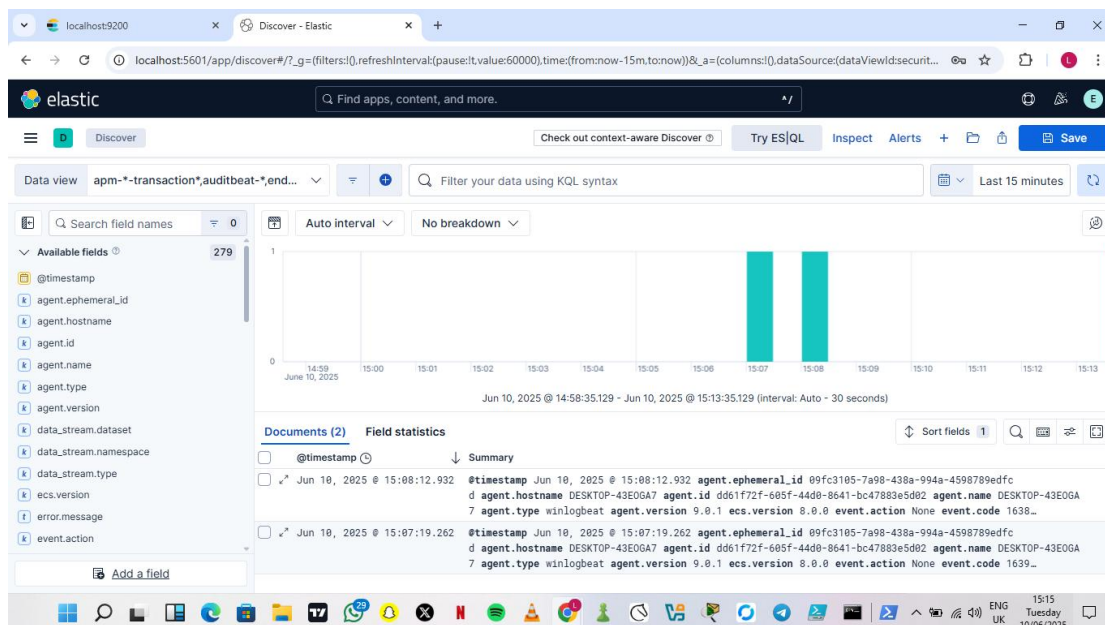
PS C:\Users\Olupelumi\Desktop\winlogbeat-9.0.1-windows-x86_64\winlogbeat-9.0.1-windows-x86_64> Start-Service winlogbeat
PS C:\Users\Olupelumi\Desktop\winlogbeat-9.0.1-windows-x86_64\winlogbeat-9.0.1-windows-x86_64> |

Completed Ln 16 Col 97 95%

```

Sysmon has been integrated successfully

**Step 4:** View sysmon event logs in ELK click on discover In the index pattern, use: winlogbeat-\* or logs-\* depending on your Winlogbeat config.and it shows the sysmon event on the pc.



Sysmon Event can be viewed on the elasticsearch setup

### What Sysmon does:

Captures logs that include rich data that's not captured by default Windows logging such as;

#### Event ID

#### What it Logs

- 1 Process creation (with command-line, hash, parent, etc.)
- 2 File creation time changes

Event ID	What it Logs
3	Network connections
6	Driver loading
7	Image (DLL) loading
10	Process access (used for detecting injection)
11	File creation
13–15	Registry key & value creation/modification
22	DNS queries
23	File deletion

### SKILLS LEARNED:

- **Configuration Management:** Used YAML and XML files to configure Winlogbeat and Sysmon. Customized logging behavior via the sysmonconfig.xml.
- **Log Forwarding & Beats Integration:** Deployed Winlogbeat to ship Windows logs to Elasticsearch. Set up and tested log pipelines between:

Sysmon → Event Log

Winlogbeat → Elasticsearch

- **Data Visualization & Analysis:** Viewing the event logs on kibana and ability to understand each event through specific event ID,

**Conclusion:** With this knowledge, I can now:

- Detect malware behavior (e.g., suspicious PowerShell, DLL injection)
- Build your own home lab SIEM
- Investigate security incidents (e.g., lateral movement, persistence)