1)We have the following files:

```
piyushg@piyushg-HP-Laptop-15g-br0xx:~/malwareproj$ ls
 agent.yml        'Four Unknown Signatures.pptx'          generatelog.sh
  netlog.txt         prometheus.yml    rungrok.sh
demoicmptcp.sh   'Four unknown Signatures report.pdf'    Malware_Project-1651257182819.json
 promAlertAPI.py    readme.pdf        server.sh
```

2)
On the server, we have a configuration file for prometheus which is **'prometheus.yml.'**
Prometheus is run using **"./server.sh"**

3) On Grafana, the dashboard has to be imported from the json file present.

3) On client, we have:

1. **agent.yml** => Configuration for grok-exporter
2. **generatelog.sh** => To start generating logs.
3. **rungrok.sh** => To run grok exporter.
4. **promAlertAPI.py** => To run the Alert Webhook which will detect attack and add iptables rule to block attackers IP.
5. **netlog.txt** => This will be generated by generatelog.sh which will be picked up by grok-exporter.

4) Installation of tools:

1. **Grafana**: Using apt install grafana.

```
root@piyushg-HP-Laptop-15g-br0xx:/home/piyushg/malwareproj# apt install grafana
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
  grafana
```

2. **Prometheus**:
   It can be downloaded and set up from here:
   https://linuxhint.com/install-prometheus-on-ubuntu/
3. **TCPDump**: Using apt install tcpdump
4. **Grok-Exporter**: Using the github repository: https://github.com/fstab/grok_exporter

5) Running:

1. ./server.sh
2. sudo systemctl start grafana
3. On client: ./rungrok.sh
4. On client: ./generatelog.sh
5. On client: ./promAlertAPI.py
6. The parameters need to be changed for Ip address.

Demo:
https://iitk-my.sharepoint.com/:u:/g/personal/akshay21_iitk_ac_in/Ec0UyOFly8BFkK-tFK1_ZxcBpYEmDC4tyrWGIndzN6210g?e=emMSFt
https://drive.google.com/file/d/1vsmBcbUZdJ-5zVsNcyJpXSkNb5bOGfAn/view?usp=sharing