Systems Infrastructure and Security
Assessment Brief

Module Leader:	Fiona Redmond
Assessment Title:	System Security Project
Assessment Type:	Practical
Individual/Group:	Individual
Assessment Weighting:	50%
Hand-out Date:	10th March 2025
Hand-in Date:	7th April 2025 09:00am
Mode of Submission:	Documentation to be submitted on Blackboard. Demonstration on your scheduled day. NOTE: Virtual Machines **not** to be accessed past the deadline.

Project Overview
You will create an automated protection and monitoring environment using the following tools:

- **Rocky Linux** and **Ubuntu 24.04** servers provided for this module.
- **Prometheus** for monitoring and alerting.
- **Grafana** for creating visual dashboards.
- **Fail2ban** for intrusion detection and prevention.

This project will help you understand how to collect, analyse, and visualize security data, identify potential threats, and improve system security.

Project Requirements

1. Environment Setup
You must install and configure the following tools on your Ubuntu server:

1. **Prometheus**:
   - Monitor at least **3 data sources**.
   - Create alerts to notify administrators about potential security events.

2. **Grafana**:
   - Connect Grafana to Prometheus as a data source.
   - Create **3 dashboards** to visualise security metrics.

3. **Fail2ban**:
   - Monitor login attempts (e.g., SSH).
   - Automatically block suspicious IP addresses based on predefined rules.

2. Testing and Documentation
- Simulate security scenarios (e.g., failed login attempts) to **test** your setup.
- Verify that:
  - **Fail2ban** blocks unwanted access.
  - **Prometheus alerts** are triggered correctly.
  - **Grafana dashboards** display accurate metrics.
- Include the following in your **documentation**:
  - Clear instructions for setup and configuration (with screenshots).
  - Any configuration files modified (e.g., `prometheus.yml`).
  - Observations about system security and any improvements made.
- Documentation should be clear and well-organised. Include references where necessary.

3. Demonstration

Prepare a **9-minute demo** to showcase your project, including:

- How Fail2ban protects the system.
- Prometheus metrics and alerting.
- Grafana dashboards.

Focus on **key features** that demonstrate your understanding of the project and its impact on security. Demonstrations will take place during our labs in the final week. Schedule of demoes can be found at the end of this brief. You must complete a demo for your submission to be accepted. i.e., your project will not be graded based on your virtual machines and documentation.

4. Submission

You must submit:

- A written report (via Blackboard).
- A functional system (demonstrated during your scheduled time).
- Note: Late submissions will incur penalties, and failure to demonstrate will result in no grade for the project.

Additional Details

Prometheus Configuration:

- Scrape metrics from at least 3 data sources using exporters. Examples (but not limited to):
    - **Node exporter** for CPU, memory, and disk usage.
    - **Fail2ban exporter** for login attempts and blocked IPs.
    - **Blackbox exporter** for probing of endpoints over HTTP, HTTPS, DNS, TCP and ICMP.
    - **MySQL Server exporter** for monitoring and exposing MySQL metrics
    - **Other exporters** exist for services such as web servers and email. Think about what you have installed in labs such as ClamAV, Nikto etc.
- Set up at least **2 alerts** using Prometheus Alertmanager to notify administrators of potential security events based on specific metric thresholds . Examples:
    - High number of failed login attempts.
    - Changes to critical files (e.g., /etc/passwd).
    - Consider how notifications will be sent (e.g. by email, Teams, slack channel, discord channel).

Grafana Configuration:

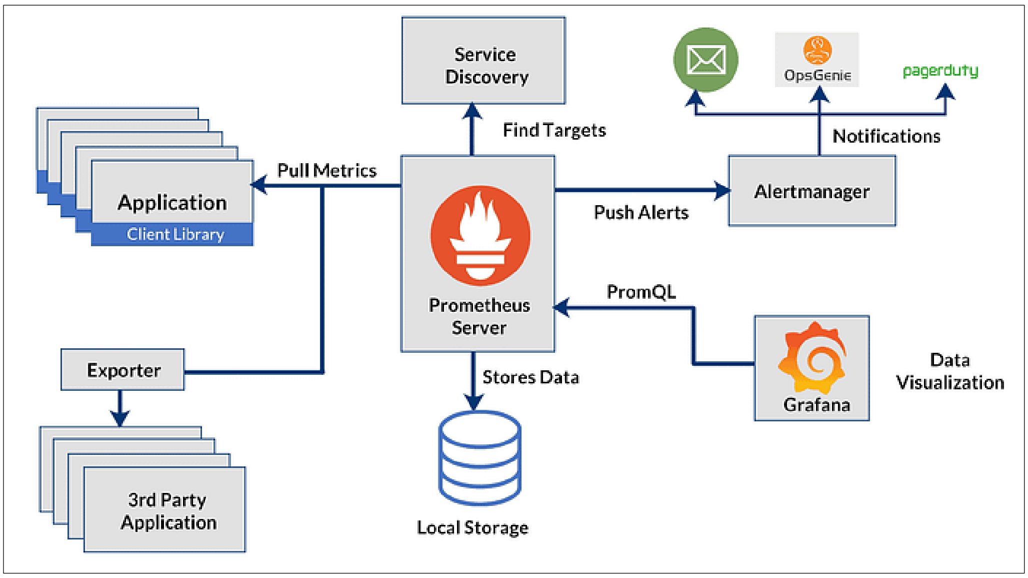
- Connect Grafana to the Prometheus server as a data source and provide real-time insights into system performance
- Create 3 dashboards to visualise metrics such as:
    - System resource usage (CPU, memory, disk).
    - Failed login attempts and blocked IPs.
    - Other security-related metrics based on your Prometheus setup.
- You can use pre-made templates (e.g. template ID 14513) or build your own.

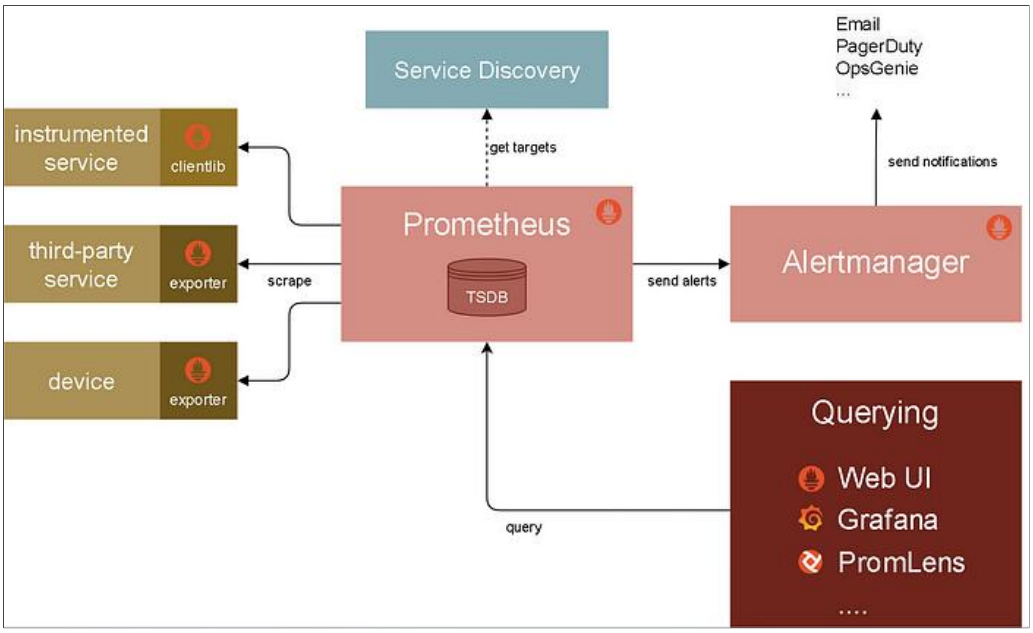
Fail2ban Integration:

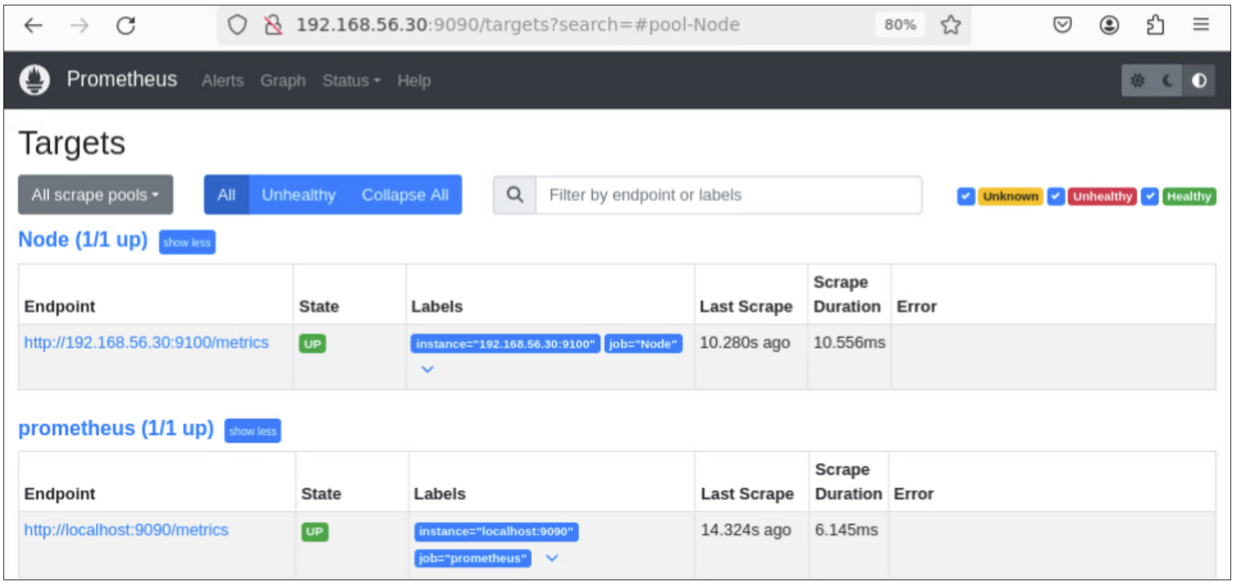
- Configure Fail2ban to monitor (detection) services like SSH or web servers.
- Set ban rules (prevention) based on criteria such as repeated failed logins.

Resources:

- https://www.fosstechnix.com/install-prometheus-and-grafana-on-ubuntu-24-04/
- https://prometheus.io/docs/instrumenting/exporters/
- https://grafana.com/docs/versions/?project=%2Fdocs%2Fgrafana%2F&pg=webinar-getting-started-with-grafana-dashboard-design-amer&plcmt=related-content-2







Targets

All scrape pools ▾ | All | Unhealthy | Collapse All | Filter by endpoint or labels | ☑ Unknown ☑ Unhealthy ☑ Healthy

Node (1/1 up) show less

Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
http://192.168.56.30:9100/metrics	UP	instance="192.168.56.30:9100" job="Node"	10.280s ago	10.556ms	

prometheus (1/1 up) show less

Endpoint	State	Labels	Last Scrape	Scrape Duration	Error
http://localhost:9090/metrics	UP	instance="localhost:9090" job="prometheus"	14.324s ago	6.145ms	

Assessment Criteria:

Breakdown	**Mark**
Functionality and Alerting: Successful installation, configuration, and integration of Prometheus, Grafana and Fail2Ban and any other selected tools. Successful implementation of useful alerts.	50
Monitoring and Visualisation: Comprehensive dashboards effectively presenting security-related metrics in Grafana.	20
Documentation: Clear and concise report outlining the project, setup steps, observed metrics, and their significance in understanding security posture.	15
Demonstration: Clarity, conciseness, and effectiveness of demonstration in conveying key project elements and insights, within allocated timeframe.	15
TOTAL	**100**

The use of any form of AI is not permitted. Your submission must be your own work and your own words. This assignment is subject to SETU's policy on plagiarism.

Notes for Demonstration Days

- **Stick to Your Time Slot:**
  - Please adhere to the scheduled time allocated to you for your demo.
- **Attendance:**
  - You only need to attend on the day of your scheduled demo.
- **Arrive on Time:**
  - Arrive at the lab at the start of the session, regardless of your scheduled time.
  - The listed times are estimates, so you may be called earlier or later than expected.
- **Be Ready:**
  - Have your virtual machines booted, logged in, and prepared before your demo begins.
  - The schedule is tight, so delays are not allowed.
- **Using Notes:**
  - You may keep notes with command reminders or file names if needed.
  - However, relying on notes could suggest a lack of familiarity with your setup.
- **Check the Schedule:**
  - Ensure your name is listed on the schedule. If it is missing, contact me immediately to be assigned a time slot.
- **Leaving the Lab:**
  - You may quietly leave the lab once your demo is completed.

Schedule of Demos on the next pages →

Cyber Group B	
Monday 7th April 9 – 10am	
9:00 – 9:10	Mateusz
9:10 – 9:20	Evan
9:20 – 9:30	Richard
9:30 – 9:40	Max
9:40 – 9:50	Jack
9:50 – 10:00	Killian

Cyber Group B	
Monday 7th April 11 – 1pm	
11:00 – 11:10	Katie
11:10 – 11:20	Abdelmoumen
11:20 – 11:30	Raluca
11:30 – 11:40	Dylan
11:40 – 11:50	Eduardo
11:50 – 12:00	Cathal
12:00 – 12:10	Melissa
12:10 – 12:20	Alwyn
12:20 – 12:30	Lloyd
12:30 – 12:40	Filip
12:40 – 12:50	Arsen
12:50 – 1:00	

Cyber Groups A & B Book C305	
Monday 7th April 3 – 4.30pm	
3:00 – 3:10	Dominik
3:10 – 3:20	Ivan
3:20 – 3:30	Antonio
3:30 – 3:40	Samuel
3:40 – 3:50	Jamie W
3:50 – 4:00	Shaafin
4:00 – 4:10	Vladyslav
4:10 – 4:20	Dawid
4:20 – 4:30	

IT Management	
Tuesday 8th April 10 – 12pm	
10:00 – 10:10	Alise
10:10 – 10:20	Christopher
10:20 – 10:30	Anthony
10:30 – 10:40	Ian
10:40 – 10:50	Omoniyinoluwa
10:50 – 11:00	Fareedat
11:00 – 11:10	Robert
11:10 – 11:20	Kim

11:20 – 11:30	Daniel
11:30 – 11:40	Adam

Cyber Group A	
Thursday 10th April 1 – 2pm	
1:00 – 1:10	Shehab
1:10 – 1:20	Timofei
1:20 – 1:30	Emily
1:30 – 1:40	John
1:40 – 1:50	Jamie D
1:50 – 2:00	Eoghan

Cyber Group A	
Thursday 10th April 3 – 5pm	
3:00 – 3:10	James
3:10 – 3:20	Munzer
3:20 – 3:30	Jolanta
3:30 – 3:40	Keith
3:40 – 3:50	Matthew
3:50 – 4:00	Jay
4:00 – 4:10	Marina
4:10 – 4:20	Petr
4:20 – 4:30	Anna
4:30 – 4:40	Tomas
4:40 – 4:50	Oisin
4:50 – 5:00	