

PROJECT OVERVIEW & PLANNING REPORT

- **Project Title : A Red team-Blue team Security Simulation on Microsoft (Major project)**
- **Your Name : Avinash Das ManikPuri**
- **ERP: 6604666**

1. Overview

This project titled "**Attack, Detect & Secure the Cloud Environment**" is a hands-on cybersecurity implementation conducted on **Microsoft Azure**. The project simulates a real-world enterprise cloud environment and follows a **Red Team vs Blue Team** methodology to identify, detect, and mitigate cyber threats.

The infrastructure consists of multiple Linux-based virtual machines representing internal systems, web-facing services, and a centralized SIEM server.

2. Objective

The primary objective of this project is to demonstrate the complete cybersecurity lifecycle in a cloud environment by:

- Simulating real-world cyber-attacks
 - Detecting malicious activities using SIEM
 - Investigating security incidents
 - Applying security hardening techniques
 - Validating security improvements through re-attack
-

3. Project Scope

3.1 In-Scope

- Azure Virtual Machine deployment
- Linux system security assessment
- Network access control evaluation
- Attack simulation and detection
- Security hardening and validation

3.2 Out-of-Scope

- Paid security tools

- Production-grade high availability systems
 - Cloud-native paid security services
-

4. Cloud Architecture Overview

The project architecture consists of the following components:

- **VM-Internal** – Internal Linux server
- **VM-Web** – Web server hosting Apache/Nginx
- **VM-SIEM** – Centralized SIEM server (Wazuh)

All systems are deployed within a single Azure Virtual Network.

AZURE DASHBOARD

The screenshot shows the Microsoft Azure dashboard for the project 'Avinash das manikpri (Dashboard)'. The left sidebar lists various Azure services: Home, Dashboard, All services, Favorites, Application Templates, All resources, Resource groups, App instances, Function App, Azure SQL Database, Azure Cosmos DB, Virtual machines, Load balancers, Storage account, Virtual network, Network Watcher, Monitor, Advisor, and Microsoft Defender for Cloud. The main area displays a summary card with the message 'Get started An environment with a virtual machine and new Azure storage. Go to classic' and a link to 'Create'. Below the card is a table titled 'Resources' showing 11 items:

Resource	Type	Region
5e944665-ac91-477f-8c7e-ef	Virtual machine	Central India
5e944665-ac91-477f-8c7e-ef	Virtual machine	Central India
5e944665-ac91-477f-8c7e-ef	Virtual machine	Central India
5e944665-ac91-477f-8c7e-ef	Network security group	Central India
5e944665-ac91-477f-8c7e-ef	Public IP address	Central India
5e944665-ac91-477f-8c7e-ef	Network Interface	Central India
5e944665-ac91-477f-8c7e-ef	Public IP address	Central India
5e944665-ac91-477f-8c7e-ef	Network Interface	Central India
5e944665-ac91-477f-8c7e-ef	Network security group	Central India
5e944665-ac91-477f-8c7e-ef	Public IP address	Central India

5. Tasks to Be Completed

1. Red Team attack simulation
 2. Blue Team investigation and detection
 3. Security hardening and mitigation
 4. Post-hardening re-attack and validation
-

Screenshot Evidence Table – Project Setup

Screenshot No.	Description	Remarks
1	Azure Resource Group Creation	Account name visible
2	Virtual Machines Overview	All VMs listed
3	Network Configuration	VNet & NSG
