**Project Title:** Detection and Mitigation of DoS/DDoS Attacks in Virtualized Cloud Environments

**Project Group Members:** [List group members and their emails here]

**Project Approach:**

**\*\*Introduction\*\***

Cloud computing provides on-demand resources via different service models, including Infrastructure as a Service (IaaS). This project aims to analyze the security challenges within cloud-based virtualized environments by exploring Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks on virtual machines (VMs) and containers. We will implement a detection and mitigation framework to secure these environments effectively.

**Project Scope and Objectives**

1. **Conduct Four DoS/DDoS Attacks:**
   * **Network-based attack on a VM** (e.g., SYN flood, UDP flood) **\*\*SYN**
   * **Host-based attack on a VM** (e.g., resource exhaustion, fork bomb) **\*\*Process**
   * **Network-based attack on a container** (e.g., ARP spoofing, DNS amplification)
   * **Host-based attack on a container** (e.g., excessive process spawning)
2. **Develop a Monitoring Tool:**
   * Implement a Python-based tool to collect system performance metrics (CPU, memory, network traffic, etc.). **\*\*modify capstone**
   * Store monitoring data in a structured database (e.g., MySQL, PostgreSQL, or MongoDB). **\*\*modify capstone**
3. **Create an Attack Detection Mechanism:**
   * Design detection rules and logic based on predefined thresholds/statistical patterns. **\*\*modify capstone**
   * Implement real-time analysis to identify abnormal activities. **\*\*modify capstone**
4. **Implement Automated Mitigation Measures:**
   * Once an attack is detected, execute countermeasures such as:
     + Adjusting firewall rules dynamically
     + Throttling or blocking malicious traffic **\*\*SYN**
     + Terminating rogue processes **\*\*Process**
     + Isolating affected containers or VMs
5. **Project Deliverables:**
   * A detailed project report covering methodology, findings, and effectiveness of mitigation strategies.
   * A live demo showcasing attack scenarios, detection, and response mechanisms.

**Implementation Plan**

**Phase 1: Research and Environment Setup (Weeks: )**

* Review existing DoS/DDoS attack methodologies and security mechanisms.
* Set up a cloud environment with a VM and container for testing.
* Select and install attack toolsets (e.g., LOIC, Hping3, Metasploit, etc.).

**Phase 2: Attack Implementation (Weeks: )**

* Execute the four attack types on the target VM and container.
* Document impact and collect relevant metrics.

**Phase 3: Monitoring Tool Development (Weeks: )**

* Develop a Python-based tool to collect system logs and performance data.
* Store monitoring data in a database for real-time and historical analysis.

**Phase 4: Detection Mechanism (Weeks: )**

* Implement and test rule-based detection algorithms.
* Fine-tune detection thresholds based on observed attack behavior.

**Phase 5: Automated Mitigation Strategies (Weeks: )**

* Develop automated responses based on detected attack patterns.
* Test effectiveness of countermeasures and adjust as needed.

**Phase 6: Final Report and Demo Preparation (Weeks: )**

* Prepare final documentation, summarizing methodology, analysis, and results.
* Conduct a live demonstration of attack, detection, and mitigation process.

**\*\*Conclusion\*\***

This project will provide practical insights into securing cloud environments by identifying, detecting, and mitigating DoS/DDoS attacks. The research and implementations will contribute to understanding proactive defense mechanisms in virtualized cloud infrastructures.