


# Cloud Blazers

William Austin, Andrew Balfour, Jeremy Crown,  
Trina Lin, and Ahmedur Rahman Shovon

A dark blue diagonal gradient bar that starts from the bottom left corner and extends towards the top right corner, covering the bottom half of the page.

# Main Idea: Cloud-Based Penetration Scanning

- Scan a large range of addresses
- Utilize multiple VMs in parallel reducing scan time and analysis
- Require authentication using cloud database technologies
- Expose vulnerabilities associated with the network (ports, OS, etc)
- Mitigation tool for developers to slow down the attacker



# Technical Approach



**NMAP**

**SSLyze**

TOOL FOR ANALYSING SSL/TLS CONFIGURATIONS

Scanning tool:

- Nmap - "Network Mapper" open source tool for network discovery & security auditing
- Sublist3r - Subdomain listing tool
- SSLyze - SSL/TLS scanning tool
- TLS-Parser - Parse TLS information
- Requests - Gather metadata from the hosts

**Sublist3r**



# Technical Approach (Cont.)

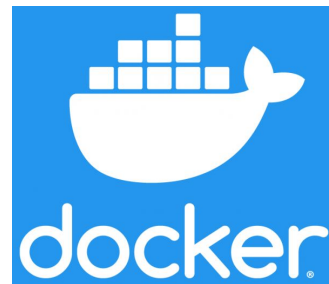


## Web application:

- Python & Flask - Provides REST APIs for concurrent scanning from multiple VMs
- SQLAlchemy - SQL Object Relational Mapper
- Cryptography - Used for cryptographic algorithms and encryptions/decryptions
- Dotenv - Sets environment variables based on the development or production environment
- Bootstrap & jQuery - Used for developing responsive frontend
- Docker with docker-compose - Creates docker containers for OS independent execution

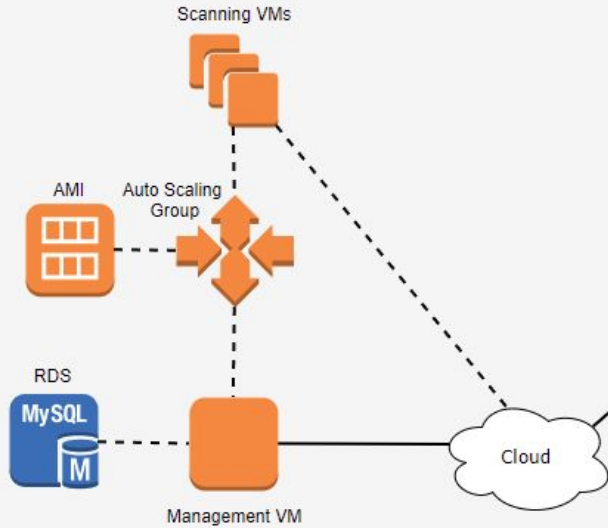


Flask



# Diagram

## Project VMs in the Cloud

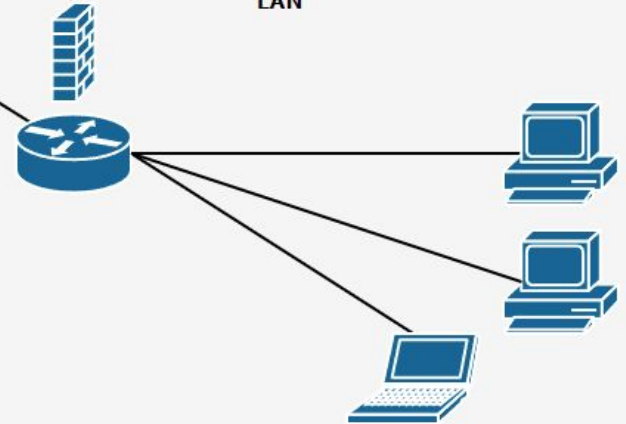


## Some Public IP Space



Internet

## LAN



EC2 > Auto Scaling groups

**Auto Scaling groups (1)** Refresh Edit Delete Create an Auto Scaling group

<input type="checkbox"/>	Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
<input type="checkbox"/>	CBPen	CBPen   Version 2	3	-	3	3	6	us-east-2b

- EC2 Dashboard New
- Events New
- Tags
- Limits
- INSTANCES
- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts New
- Scheduled Instances
- Capacity Reservations
- IMAGES
- AMIs
- ELASTIC BLOCK STORE
- Volumes
- Snapshots
- Lifecycle Manager
- NETWORK & SECURITY
- Security Groups New
- Elastic IPs New
- Placement Groups New
- Key Pairs New
- Network Interfaces

# Lessons learned/discussion

- Additional Pentesting Tools
- Scalability
  - AWS Auto Scaling (Elastic IPs), Elastic Beanstalk
- Scanning Through Proxy
- 2FA login system (Amazon Cognito)
- Password Reset
- Condensing libraries and tools

# Task Distribution

William Austin: Meeting organizer and research additional project options for scaling (Elastic Beanstalk) & scanning (Wireshark).

Andrew Balfour: Flask development with nmap OS scanning. Creation of the login page and database, including SQLite to MySQL migration.

Jeremy Crown: Implemented, updated, and maintained VMs, autoscaling group, and RDS instance in AWS.

Trina Lin: Updated Contacts and Terms & Conditions pages and researched AWS Elastic Beanstalk and Auto Scaling.

Ahmedur Rahman Shovon: Developed backend (REST APIs) and frontend (monitor app) of the web application accommodating scanning tools in EC2.