Week 12: Final Presentation and Submission

Name- Saish Dhiwar
PRN- 2124UCSM2011
Email- saish.dhiwar_24ucs@sanjivani.edu.in

Program: DIY Internship – Cloud Security Fundamentals & Incident Response

Duration: 12 Weeks (June – August 2025)
Objective: To gain hands-on knowledge of cloud security concepts and incident response processes.

Key Focus Areas

1. Cloud environment setup (AWS/GCP)
2. Identity and Access Management (IAM)
3. Cloud storage security
4. Logging & monitoring (CloudTrail, CloudWatch)
5. Network security and WAF configuration
6. Vulnerability scanning & remediation
7. Data encryption (at rest & transit)
8. Cloud compliance and auditing
9. Incident response handling
10. Final audit & reporting
11. Documentation & GitHub management
12. Final presentation & submission

Deliverables

1. Weekly task documentation with screenshots.
2. Security audit & compliance reports.
3. Final presentation video and GitHub repository submission.

Internship Overview

Cloud Platforms: AWS (EC2, S3, IAM, CloudTrail, WAF, Config, Inspector, RDS, EBS)
Security Tools: Cloudflare, Amazon Inspector, AWS Config
Monitoring Tools: CloudWatch, CloudTrail

Weekly Tasks

Week 1 – Cloud Environment Setup

- Created an AWS Free Tier account.
- Launched EC2 instance (Ubuntu, t2.micro).
- Configured key pairs, security groups, and SSH access.
- Documented setup in GitHub with screenshots.

Week 2 – Identity and Access Management (IAM)

- Created IAM **users, groups, and roles**.
- Assigned permissions via policies.
- Attached EC2S3ReadOnlyRole to instances.
- Implemented the principle of least privilege.

Week 3 – Cloud Storage Security

- Configured S3 bucket with access policies.
- Enabled **SSE-S3 encryption** for data at rest.
- Restricted public access and applied bucket policies.
- Enabled versioning and logging for auditability.

Week 4 – Logging & Monitoring

- Enabled **CloudTrail** to capture account activity.
- Stored logs in a dedicated S3 bucket.

- Integrated with **CloudWatch Logs** for alerts.
- Created alarms for suspicious activities (e.g., `AccessDenied` errors).

Week 5 – Network Security

- Configured EC2 **Security Groups** and firewall rules.
- Allowed only required ports (22/80/443).
- Blocked unnecessary ports to reduce the attack surface.
- Documented final security ruleset in GitHub.

Week 6 – Web Application Firewall (WAF)

- Configured **AWS WAF** with CloudFront distribution.
- Applied AWS Managed Rule Sets (SQLi, XSS, Bot Control).
- Tested with malicious payloads → requests blocked (403).
- Documented configuration and screenshots.

Week 7 – Cloud Vulnerability Scanning

- Used **Amazon Inspector** to scan EC2 instances.
- Identified vulnerabilities (outdated OpenSSL, Apache).
- Applied remediation via patching and updates.
- Verified fixes by re-scanning instances.

Week 8 – Simulated Attack & Incident Response

- Created IAM user `compromised-user` with limited S3 access.
- Generated access keys and attempted unauthorized actions (delete object, terminate EC2).
- Detected anomalies via **CloudTrail Event History**.
- Response actions: deactivated access keys, removed permissions, enforced MFA.

Week 9 – Data Encryption (At Rest & Transit)

- Enabled encryption on **S3 (AES-256 SSE-S3)**.
- Created **encrypted EBS volumes** with KMS keys.
- Enabled RDS encryption for the database.
- Configured **HTTPS (TLS/SSL)** using Certbot on EC2 web server.

Week 10 – Cloud Security Compliance Check

- Enabled **AWS Config** to track compliance.
- Applied managed rules (`s3-bucket-encryption-enabled`, `ec2-no-public-ip`, `iam-mfa-enabled`).
- Identified misconfigurations: unencrypted S3, public EC2 IP, and missing MFA.
- Remediated issues → all rules showed `COMPLIANT`.

Week 11 – Final Cloud Security Audit

- Reviewed all AWS resources.
- Misconfigurations found: open SSH port, unused IAM keys, unencrypted S3.
- Fixed by restricting SGs, deleting keys, and enabling encryption.
- Prepared final audit report (COMPLIANT status achieved).

Week 12 – Final Presentation & Submission

- Submitted **GitHub repository** with:
    - Weekly task documentation
    - Final presentation PPT
    - Final Report
- Completed full internship submission.

Key Learnings

- **IAM & Access Control** → Importance of least privilege, MFA, key rotation.
- **Cloud Logging & Monitoring** → Proactive alerts with CloudTrail + CloudWatch.
- **WAF & Network Security** → Protecting apps against OWASP Top 10 threats.
- **Vulnerability Management** → Using Amazon Inspector and patching.
- **Data Encryption** → Securing data at rest and in transit with KMS & TLS.
- **Compliance & Audit** → Continuous monitoring with AWS Config.
- **Incident Response** → Simulated attack handling & rapid remediation.
- **Documentation & Reporting** → Professional GitHub repository with reports, screenshots, and video.

Conclusion

Successfully completed a 12-week DIY Internship on Cloud Security Fundamentals & Incident Response.

- Gained practical knowledge of cloud security controls, monitoring, and compliance.
- Learned to detect, respond, and remediate cloud incidents.
- Secured AWS resources using IAM, encryption, logging, monitoring, and auditing.
- Developed strong documentation and reporting skills for professional presentation.

This internship prepared me for real-world cloud security challenges and advanced certifications in AWS Security & Cloud Compliance.
