**Task 2 - Tools and Documentation**

1. Identify tools that will allow you to do the following: a. Scan infrastructure as code templates. b. Scan AMI’s or containers for OS vulnerabilities. c. Scan an AWS environment for cloud configuration vulnerabilities.
2. For each tool - identify an example compliance violation or vulnerability which it might expose.

|  |  |  |
| --- | --- | --- |
|  | Tools | Vulnerability Expose |
| Scan infrastructure as code templates | * Prisma cloud * Security Hub * Cloud Sploit * Accurics * Terrafirma * TFLint * Checkov | * Cloud misconfigurations. * Static Code analysis |
| Scan AMI’s or containers for OS vulnerabilities | * AWS Inspector * Anchore * Clair * Dagda * Sysdig Falco | * Common Vulnerabilities and Exposures (CVE) * Allowing SSH password login |
| Scan an AWS environment for cloud configuration vulnerabilities | * Aws Config * InsightVM | * IAM Role with Administration Access * Disk Volume with No Encryption * Instance SG Allows RDP from Internet |