MODULE 8

Praneesh Sharma

21052264

**AWS Sheid:** A managed DDoS protection service that safeguards applications running on Amazon Web Services (AWS).

**AWS WAF:** A service that gives you control over which traffic to allow or block to your web applications by defining customizable web security rules.

**Distributed denial of service (DDoS):** A malicious attempt to make a targeted system, such as a website or application, unavailable to end users. To achieve this, attackers use a variety of techniques that consume network or other resources, interrupting access for legitimate end users.

**Amazon Inspector:** An automated security assessment service. It helps you test the network accessibility of your Amazon Elastic Compute Cloud (Amazon EC2) instances and the security state of your applications running on the instances.

**AWS Artifact:** A central resource for compliance-related information. It provides on-demand access to AWS security and compliance reports and select online agreements.

Four areas of security must be addressed for cloud computing:

* Data: Protecting the information that is stored and processed in the cloud
* Permissions: Regulating who has access to the resources and data in the cloud
* Infrastructure: Protecting the machines and hardware that run. store, and process data in the cloud
* Assessment: Inspecting the infrastructure, permissions, and data to make sire they are secure.

Shield and AWS WAF are services that address attacks on infrastructure, primarily the network used to access cloud resources. Amazon Inspector addresses assessment by investigating how well the cloud resources we use, such as our EC2 instances, are being protected. It also investigates whether these resources are following best practice guidelines.

One major type of cyberattack is called a DDoS. A DDoS occurs when attackers set up programs that send thousands or millions of requests to an app, website, or service at the same time. This spike in traffic can consume resources to the point where the website or app is no longer accessible for legitimate users. DDoS attacks can be done for many reasons including competition, political motivation, or economic motivation.

****Shield**** works in conjunction with Elastic Load Balancing, Amazon CloudFront, and Amazon Route 53 to protect against DDoS attacks. There are 2 tiers of service:

* AWS Shield Standard is available to all AWS users at no extra cost. It protects users from the most common DDoS attacks. This protection is applied automatically and transparently to any ELB resources, CloudFront distributions, and Route 53 resources.
* AWS Shield Advanced provides additional DDoS mitigation capability for volumetric attacks, intelligent attack detection, and mitigation for attacks at the application and network layers. Users get 24/7 access to the DDos Response Team (DRT) for custom mitigation during attacks. Users also get advanced real-time metrics and reports, and DDoS cost protection to guard against bill spiked in the aftermath of a DDoS attacks. Shield Advanced is available at an additional cost.

**AWS WAF** is another defensive tool provided by AWS. It helps protect web applications from exploits that might affect availability or security or consume resources. AWS WAF can monitor an application’s web traffic and decide which traffic to let through based on specific request being made. AWS users can create their own set of rules to direct what traffic is allowed by AWS WAF to specific IP addresses.

**Amazon Inspector** does not actively protect your AWS services. Instead, it monitors the services and gives you updates on any vulnerabilities or any place where you are not following best practices. This can be useful to experts to make sure they are meeting security compliance standards and for new user who can learn about best practices.

Amazon Inspector security assessments help you check for unintended network accessibility of your EC2 instances and for vulnerabilities on those EC2 instances. Amazon Inspector assessments are offered to you as predefined rules packages mapped to common security best practices and vulnerability definitions. Examples of built-in rules include checking for access to your EC2 instances form the internet, remote root login being activated, or vulnerable software versions installed. AWS security researchers regularly update these rules.

AWS Artifact is a centralized resource for compliance-related information. Different organizations require cloud service providers (CSPs) to meet many different certifications and rules to host their data or process requests. Organizations that handle sensitive data such as bank information, personal information, or medical records must ensure that their cloud service meets certain security standards. AWS Artifact lists and gives details about the different compliance standards they meet.