3 tier architecture

SYN Flood Attacks

Disaster Recovery

Server Hardening

Cloud Deployment model and Service model

Shared Responsibility models for IaaS, PaaS, SaaS

IAM users vs roles

Identity-based vs resource-based polcies

Different encryption keys

ACM Cert Signing process

Focus areas of sec ops

Cloud trail vs CloudWatch

Phases of incident response

**Week 7**

Purpose of secops is to detect, respond to, and recover from active attacks on enterprise assets

As sec ops mature:

1. Reactively respond to attacks that are detected by tools
2. Proactively hunt down attacks that have slipped past tools

Logging is the collection and recording of activity and event data

Info logged depends on service, service can provide logging or may be outsourced to secondary service. Commonly logged = Date and time of event, Origin of event, Identity of resources accessed

Benefits of logging:

1. Troubleshooting
2. Auditing
3. Bookeeping
4. Incident response and remediation

Monitoring is the continuous verification of the security and performance of the resources, applications, and data.

CloudTrail is used for logging , CloudWatch for monitoring.

CloudTrail enables governance and compliance and operational and risk auditing for your AWS account. Used to view, analyze and respond to account activity across the AWS infrastructure

API-Security Relevant information include:

1. Name of the API
2. Identity of the caller
3. Time of the API call
4. Origin location of request
5. Request parameters
6. Response elements

Week 1 Recap

Server Roles

A server is a computer that responds to requests from other computers. It is used in a client-server model, peer to peer models have no servers. Servers can be used for different purposes

1. Web server
   1. Shows info to users when they connect to the server using a web browser which is the client part of the application
   2. HTTP/HTTPS as its transfer mechanism
2. Application server
   1. Contains most of the business logic and is the middle tier in the 3-tier architecture
   2. Users connect to to run their applications on
   3. Comms with db server where content is stored
3. Database server
   1. Contains database software such as SQL. Holds info stored in db, accesssed by users through application GUI or command line instructions
4. File server
   1. Server that stores and holds files that can be accessed by network users
5. Network services server DHCP
   1. Automates the process of assigning an IP address to computers that join the network
6. Network services server DNS
   1. Resolves linking domain names and ip addresses
7. Directory services server
   1. Accepts and verifies the credential of users.
   2. Active Directory and Domain Services (AD DS)
   3. Acts as the core directory service, managing hierarchical rs between network objects.

Server Attack Vectors

1. Weak username and password
   * + Most common type of access credential
     + Exposes in data leaks, phishing scams, malware
     + Gives attackers access
     + Use 2FA, MFA, biometrics, password managers to counter
2. Poor encryption
   * + Must have strong encryption for data-at-rest and data-in-transit
     + SSL certs can prevent MITM attacks and protect the confidentiality of data being transmitted
3. Denial of Service
   * + Prevent a system from responding to legitimate traffic for resources
     + Common to have attacks that transmit so many data packets the server cannot process them all
     + Or exploit a known fault or vulnerability in an OS or app
     + Results in a system crash / 100% utilization
   1. Botnets
      * Set of computers that haven been infected by a control program called a bot
      * Attackers can use these computers to mount attacks
      * Such as DoS attacks, spam email, mine for passwords
      * Users of these zombies often unaware of it
   2. SYN Flood
      * A half open attack
      * Exploits the fact that the server will wait for the final final ACK packet in the handshake
   3. Ping Flood
   4. Ping of Death
   5. DDOS