Software and Systems Security

Domain 2.0

Security Solutions for Infrastructure Management

Chapter 8

Episode 8.01

Network Architecture and Asset Management

Objective 2.1 Given a scenario, apply security solutions for infrastructure management.

- Asset management
  - Asset tagging
- Network architecture
  - Physical
  - Software-defined
  - Virtual private cloud (VPC)
  - Virtual private network (VPN)
  - Serverless

Network Architecture

- Physical
  - Star
  - Bus
  - Mesh
- Software-defined
  - Control layer (routing)
  - Data layer (moving packets)

Network Architecture

- Virtual private cloud (VPC)
  - Private resources in a public cloud environment
  - Uses encryption for security
- Virtual Private Network (VPN)
  - Secure tunnel between two endpoints
  - Almost always encrypted
- Serverless
  - Deploy software network components without a server
  - FaaS
  - Use other peoples' services instead of hosting your own

Asset Management

- IT Asset Management (ITAM)
- Asset lifecycle
  - Acquisition
  - Deployment
  - Maintenance
  - Retirement
  - Disposal
- Maintaining inventory and configuration
  - Asset tagging

Episode 8.02

Protecting Your Territory

Objective 2.1 Given a scenario, apply security solutions for infrastructure management.

- Segmentation
  - Physical
  - Virtual
  - Jumpbox

Network Segmentation

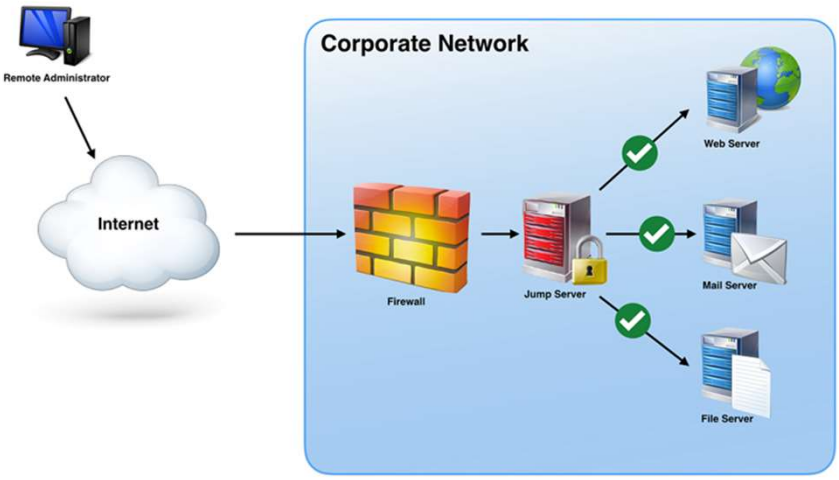
- What is network segmentation?
  - The process of breaking down large networks into smaller networks/zones
- What does it do?
  - Improves management of network
  - Improves traffic across network
  - Prevents attacker from moving across networks

Network Segmentation

- Achievable across all OSI & TCP/IP layers
- Physical layer segmentation
  - Separate networks & devices connected to separate interconnecting devices
- Link layer segmentation
  - VLANs allows multiple devices across multiple networks to be connected to the same physical device
    - Manage traffic
    - Ensure segmentation
    - Verify hard isolation across networks

Jump Box/Server

- Channelizing
- Monitoring



Episode 8.03

Identity and Access Management

Objective 2.1 Given a scenario, apply security solutions for infrastructure management.

- Identity and access management
  - Privilege management
  - Multifactor authentication (MFA)
  - Single sign-on (SSO)
  - Federation
  - Role-based
  - Attribute-based
  - Mandatory
  - Manual review
- Cloud access security broker (CASB)

Identity and Access Management (IAM)

- Determining a user's identity
  - Identification
  - Authentication
- Managing identities
- Process
  - Register as new user
  - Provide credentials
  - Authentication
    - Password, PIN, token, biometrics, etc.

Identity and Access Management (IAM)

- Privilege management
  - Authorization
    - Providing resource access
  - The key is authentication
    - Multifactor authentication (MFA)
- Single sign-on (SSO)
  - Using a single identity across several applications or organizations
  - Security Assertion Markup Language (SAML)
    - Manages and transports SSO credentials

Identity and Access Management (IAM)

- Federated identification
  - Using a single identity across several organizations
  - User identifies/ authenticates with a central identity manager
  - Example: OpenID

IAM Methods

- Role-based access control (RBAC)
  - Users (subjects) belong to one or more roles (groups)
  - Object permissions are granted based on role
- Attribute-based access control (ABAC)
  - Users (subjects) possess descriptive attributes
  - Object permissions are granted based on attributes
- Mandatory access control (MAC)
  - Subjects have clearances
  - Objects have classifications

IAM Auditing

- Manual review
  - Necessary to identify malicious behavior

Cloud Access Security Broker (CASB)

- CASB runs between users and cloud services
- Four CASB pillars
  - Visibility – subject/object access transparency
  - Threat protection – detects and blocks malicious activity
  - Compliance – controls to adhere to regulatory requirements
  - Data security – controls to protect sensitive data

Episode 8.04

Encryption and Active Defense

Objective 2.1 Given a scenario, apply security solutions for infrastructure management.

- Honeypot
- Encryption
- Certificate management
- Active defense

Encryption

- Mathematical technique to scramble text
  - Converts plaintext into ciphertext
  - Reversable (converts ciphertext into plaintext)
- Types of encryption
  - Symmetric (private key)
  - Asymmetric (public key)
- Public-key cryptography (asymmetric encryption)
  - Uses two keys
    - Public and private key pair
  - If you encrypt with one key, you can decrypt with the other

Digital Signature

- Uses encryption
- Uses hashing
  - Mathematical function that take input and creates a unique fixed-length output
- Verifies the message sender

Certificate Management

- Digital certificate
  - Public key of a known identity
  - Stored by a trusted entity
- Certificate authority
  - Trusted entity that stores public keys of known identities
- Trust is the foundation

Certificate Management

- X.509
  - IEEE certificate standard
  - Defines certificate contents
- Certificate management includes
  - Creation
  - Authenticating
  - Storage (trusted)
  - Distribution
  - Revocation

Active Defense

- Avoid being a sitting target
- Moving Target Defense (MTD)
  - Change attack surface frequently to confuse attackers
  - Honeypots and honeynets
- Use obfuscation and agility
  - Reduces value of reconnaissance