Day 8

"CLOUD SECURITY"

Shared Responsibility in Network Virtualization Security:

1. **Cloud Provider Responsibilities**
    - Implement secure, segregated network infrastructure.
    - Prevent packet sniffing, ensure tenant isolation, and enable built-in firewalls.
    - Protect SDN metadata, and detect/mitigate virtualization-level attacks.
2. **Cloud User Responsibilities**
    - Properly configure virtual networks and firewalls.
    - Use immutable templates for safe, repeatable setups.
    - Manage user rights and secure management plane controls.

Security Benefits of Software-Defined Networking (SDN):

1. **Centralized Control & Flexibility**
    a. SDN separates control and data planes, allowing centralized, dynamic policy enforcement.
    b. Admins can block or prioritize packets and manage multiple isolated networks with ease.
2. **Enhanced Visibility & Management**
    a. Central controller provides full network visibility and centralized rule deployment across virtual/physical switches.
    b. Allows real-time traffic monitoring and quick deployment of security responses.
3. **Cost & Resource Efficiency**
    a. Supports hardware/service virtualization, lowering costs and physical constraints.
    b. Reduces hardware footprint and operational complexity, while enabling scalable, secure cloud networking.

Network Component Security Considerations in Cloud:

1. **Understand Provider Security & Review Certifications**
    - Know what security your cloud provider ensures under the shared responsibility model.
    - Regularly review cloud-specific certifications and attestations to verify compliance and best practices.
2. **Use SDN & Isolate Networks**
    - Prefer Software-Defined Networking (SDN) for enhanced segmentation and control.
    - Isolate virtual networks and accounts to reduce the impact of potential breaches (blast radius).
3. **Implement Granular Firewall Controls**
    - Apply default-deny cloud firewalls, allowing only trusted IPs.
    - Use security groups per workload, not per network, and avoid heavy reliance on virtual appliances due to scalability issues.

Compute Component Security in Cloud:

1. **Dynamic Scaling & Isolation**
    - Compute instances should auto-scale as per app demands.
    - Use hypervisor-level isolation to keep instances on the same host securely separated.
2. **Data & Memory Protection**
    - Reset storage blocks before reuse to prevent data leakage.
    - Scrub unused memory before reallocating it to new instances.
3. **Layered Security & Authentication**
    - Apply multi-level security (host OS, guest OS, firewall).
    - Enforce multi-factor authentication (MFA) and use encrypted file systems for extra protection.

Container Security Essentials:

1. **Foundational Security**
    - Secure the underlying physical infrastructure, host OS, and container engine.
    - Protect the management plane with RBAC and strong authentication.
2. **Image & Repository Protection**
    - Use secure container registries with access controls to store only trusted images.
    - Enforce secure configurations and validate container images before deployment.
3. **In-Container Security**
    - Configure task/code security inside containers.
    - Understand and control namespaces, port mappings, memory/storage access for isolation.

Virtual Machine (VM) Image Security Best Practices:

1. **Encryption & Hashing**
    - Encrypt VM images before storage and during backup to prevent unauthorized access.
    - Use hashing to verify image integrity and detect tampering or corruption.
2. **Patching & Updates**
    - Always apply the latest security patches and updates to the base VM images before deployment.
3. **Backups & Recovery**
    - Perform regular backups of VM images and ensure those backups are encrypted for secure recovery.

--The End--