Troubleshooting Security Issues

6.3 Given a scenario, troubleshoot security issues

Description

- In this episode, we will explore common cloud security issues as well as strategiesv to detect and mitigate these types of issues.

Resources

- https://datatracker.ietf.org/doc/rfc6649/
- https://datatracker.ietf.org/doc/rfc9155/
- https://haveibeenpwned.com/

Learning Objectives

- List and describe common security issues associated with cloud environments
- List and describe common tools and techniques used to detect and mitigate cloud security issues

Notes

- Cipher suite deprecations
    - RC4 and 3DES (https://datatracker.ietf.org/doc/rfc6649/)
    - MD5 and SHA-1 (https://datatracker.ietf.org/doc/rfc9155/)
- Authorization issues
    - Privilege escalation
        - Vertical vs. Horizontal Priv Esc
        - Self Escalation
            - `iam create-policy-version -set-as-default`
        - Confused Deputy
            - User/App-A has permissions
            - User/App-B does not have permissions
            - User/App-B can request that User/App-A perform actions on their behalf
                - In AWS this can be done with the *instance-profile-attachment* permissions
                    - `aws iam add-role-to-instance-profile --instance-profile-name ec2-admin`
                    - `aws ec2 associate-iam-instance-profile --iam-instance-profile file://instance_profile.json --instance-id "xxxxx"`
                        - Attacker can now create ssh keys and a VM with admin creds
                        - Login and gain admin access to other resources
        - Accidental Inheritance
            - Easy to accidentially assign too much access through inheritence
    - Unauthorized access
    - How to detect?
        - Logging and monitoring
            - AWS CloudTrail, CloudWatch, GuardDuty
            - Azure Monitor, Azure Diagnostics, Network Watcher, PowerBI
- Authentication issues
    - Leaked credentials
        - Github Code Scanning Alerts (leaked keys)
        - Have I Been Pwned (https://haveibeenpwned.com/)
        - Dark web monitoring

- Software vulnerability issues
    - Vulnerability Assessments
        - Nessus
        - Qualys
- Unauthorized software
    - Shadow IT
    - Malware
        - Software asset audits
        - Threat hunting