Common Cloud Attacks

4.6 Given a scenario, monitor suspicious activities to identify common attacks

Description

- In this episode, we'll look over common attack types and activities. This includes attacks such as Social Engineering, Metadata Service exploits, Command and Control(C2), and Malware.

Resources

- http://level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud/243f422c/

Learning Objectives

- List and describe common attack activites such as Event Monitoring/Eavesdropping, Baseline deviations, Command and Control(C2)
- List and descrive common attack types such as system exploitation, Social Engineering, Malware, DDoS, Cryptojacking, and Metadata Services exploitation

Notes

- Event monitoring
    - A means of eavesdropping/surveillance
    - Insider threats
- Deviation from the baseline
    - Attacker-made changes
        - Software add/remove/config
        - Security modifications (AV/Logging/Firewall/etc)
- Unnecessarily open ports
    - C2
- Attack types
    - Vulnerability exploitation
        - Human error
        - Outdated software
    - Social engineering
    - Phishing
    - Malware
        - Ransomware
    - DDoS
    - Cryptojacking
        - Malicious code that hijacks target resources in order to mine cryptocurrency
    - Zombie resources
        - Forgotten cloud resources
        - Why they make you vulnerable
            - Not being patched/updated
            - Not being monitored
            - Not visible to your management and security tools
            - Not being scanned for vulnerabilities
            - Not being scanned for compliance
            - Costing you MONEY!
    - Metadata

- AWS and Azure have a metadata service
- SSRF can allow for access to the metadata services to reveal secrets
    - Example: Flaws Level 5 (http://level5-d2891f604d2061b6977c2481b0c8333e.flaws.cloud/243f422c/)
        - The proxy service is vulnerable to SSRF
            - Allowing access to Metadata Service data
                - `/169.254.169.254/latest/meta-data/identity-credentials/ec2/security-credentials/ec2-instance`