OMAR ARDID

STEVE CHEREWATI

GILBERT COLLADO

STRIDE Analysis Template:

Scope:

System/Process Name: AWS Infrastructure and Instances

Description: The AWS infrastructure includes multiple EC2 instances, all of which were subject to various security threats by a third party. The data provided includes evidence of brute force attacks, elevation of privilege, and port scanning, as detected by AWS GuardDuty and Splunk logs.

Scope: The scope of this analysis includes:

- All EC2 instances within the AWS VPC
- Network interfaces and security groups associated with these instances
- AWS services such as GuardDuty, CloudTrail, and VPC Flow Logs for monitoring and logging
- Splunk for log aggregation and analysis

STRIDE Threats:

DFD Element	Threat Category	Description of Threat	Impact Level	Likelihood	Mitigation Strategies
EC2 Instances	Spoofing	Instances could be impersonated if an attacker gains access to security credentials or keys.	High	Medium	Implement IAM roles and policies, use MFA, and regularly rotate keys.
EC2 Instances	Tampering	Attackers might tamper with data on compromised instances, altering logs, configurations, or stored data.	High	Medium	Use file integrity monitoring, implement strict access controls, and ensure proper logging and auditing.

EC2 Instances	Repudiation	Users might deny actions performed during the attack due to insufficient logging.	High	Medium	Enable detailed logging with CloudTrail, use immutable logs, and implement non-repudiation measures.
User Data	Information Disclosure	Sensitive information could be exposed if an attacker gains unauthorized access to the instances.	High	High	Encrypt data at rest and in transit, implement strong access controls, and monitor for data exfiltration.
EC2 Instances	Denial of Service	Brute force attacks and port scanning could lead to service outages or degraded performance.	High	High	Implement rate limiting, use AWS Shield for DDoS protection, and monitor network traffic.
EC2 Instances	Elevation of Privilege	Special privileges assigned to new logons could be exploited to gain higher access levels.	High	High	Regularly update and patch systems, use least privilege principle, and monitor privileged actions.
Network	Brute Force Attack	GuardDuty detected multiple brute force attacks on instances via RDP and WinRM.	High	High	Implement strong password policies, account lockout mechanisms, and monitor and alert on suspicious activities.
Network	Port Scanning	GuardDuty detected outbound port scans from instances, indicating potential reconnaissance activities.	Medium	High	Use network monitoring and IDS, restrict outbound traffic, and regularly

audit security group rules.

Explanation:

Spoofing:

- **Description:** Attackers could impersonate legitimate instances if they obtain security credentials, leading to unauthorized actions and access.
- **Mitigation Strategies:**
    - Implement IAM roles and policies to ensure instances only have necessary permissions.
    - Use multi-factor authentication (MFA) to protect access.
    - Regularly rotate keys and credentials to limit exposure.

Tampering:

- **Description:** Compromised instances could have their data or logs altered by attackers to hide their activities or manipulate outcomes.
- **Mitigation Strategies:**
    - Use file integrity monitoring to detect unauthorized changes.
    - Implement strict access controls to limit who can modify critical files.
    - Ensure proper logging and auditing to track changes.

Repudiation:

- **Description:** Without sufficient logging, users could deny performing malicious actions on compromised instances.
- **Mitigation Strategies:**
    - Enable detailed logging using AWS CloudTrail to track user and API activities.
    - Use immutable logs that cannot be altered after creation.
    - Implement non-repudiation measures to ensure actions are verifiable.

Information Disclosure:

- **Description:** Sensitive data could be exposed if an attacker gains unauthorized access to instances.
- **Mitigation Strategies:**
    - Encrypt sensitive data both at rest and in transit.
    - Implement strong access controls to limit who can access sensitive information.
    - Monitor for data exfiltration using tools like GuardDuty.

Denial of Service:

- **Description:** Brute force attacks and port scanning can overload instances, leading to service outages or performance degradation.
- **Mitigation Strategies:**
  - Implement rate limiting to control the flow of incoming requests.
  - Use AWS Shield for DDoS protection.
  - Monitor network traffic for unusual patterns using VPC Flow Logs and GuardDuty.

Elevation of Privilege:

- **Description:** Special privileges assigned to new logons could be exploited to gain higher levels of access within the instances.
- **Mitigation Strategies:**
  - Regularly update and patch systems to fix vulnerabilities.
  - Apply the principle of least privilege to restrict access levels.
  - Monitor privileged actions to detect unusual activity.

Brute Force Attack:

- **Description:** GuardDuty detected multiple brute force attacks targeting instances via RDP and WinRM, attempting to guess passwords to gain access.
- **Mitigation Strategies:**
  - Implement strong password policies to make passwords harder to guess.
  - Use account lockout mechanisms to temporarily disable accounts after several failed login attempts.
  - Continuously monitor and alert on suspicious activities using GuardDuty and Splunk.

Port Scanning:

- **Description:** GuardDuty detected outbound port scans from instances, indicating that attackers are looking for open ports and services to exploit.
- **Mitigation Strategies:**
  - Use network monitoring and intrusion detection systems (IDS) to detect and respond to port scanning activities.
  - Restrict outbound traffic to necessary services and ports using security groups and network ACLs.
  - Regularly audit security group rules to ensure they are properly configured.