Breaking down common attack vectors on AWS

Author: Vedang Joshi
Published: November 11, 2024 · 5 min read

With the proliferation of cloud computing, organizations are increasingly adopting services like AWS to scale their operations. However, the cloud presents unique challenges in securing assets. Notably, public IP addresses and user credentials emerge as some of the most significant attack vectors in cloud environments. This blog delves into the intricacies of these attack vectors, drawing from notable breaches to illustrate risks and explore effective mitigation strategies.

High-Profile AWS Breaches: Lessons Learned

Some major breaches underscore how severe misconfigurations and permissions issues can be within AWS and cloud environments in general. **Companies like Dropbox, Capital One, Twilio, and Mobikwik** have suffered substantial data breaches due to cloud mismanagement. Key factors in these breaches included:

- **Over-privileged IAM credentials:** Attackers often exploit excessive permissions granted to users or applications, allowing them to move laterally within a network or access sensitive data.
- **Misconfigured Firewalls:** Many organizations fail to properly restrict traffic, inadvertently exposing their services to the open internet.
- **Public S3 Buckets:** Misconfigured S3 storage buckets, accessible without authentication, have led to unauthorized access to sensitive data.

These incidents highlight critical areas in cloud security that are often overlooked, reinforcing the need for strict security configurations and continuous monitoring.

Core Attack Vectors in the Cloud: Public IP Addresses and User Credentials

1. Public IP Addresses

Public IPs allow resources to be accessible from anywhere, making them highly vulnerable if not properly secured. Key risks associated with public IPs include:

- **Exposed EC2 Instances:** Misconfigured security groups can leave EC2 instances open to the internet, making them vulnerable to attack.
- **Public S3 Buckets and RDS Instances:** Publicly accessible storage or database instances are critical vulnerabilities, especially if they contain sensitive data.

Severity Assessment:

- **Critical:** EC2 instances with misconfigured security groups are at high risk and should be secured immediately.
- **High to Low:** While public S3 buckets and RDS instances are less commonly exposed, they still represent significant risks. Public access to these services, even in test or POC environments, can lead to unintended data exposure.

2. User Credentials

Compromised credentials are one of the most frequent causes of cloud breaches. In AWS, this includes:

- **Credentials Exposed in Code Repositories:** Hard-coded credentials or secrets accidentally pushed to public repositories (like GitHub) expose systems to direct attacks.
- **Integration with Third-Party Tools:** Tools like New Relic, Databricks, and Snowflake often have API access to AWS. If these tools are compromised, attackers can pivot into AWS resources.
- **Credentials Stored on EC2 Instances or EKS Pods:** If an EC2 instance or containerized application with embedded credentials is compromised, attackers gain access.
- **Weak Credentials in Communication Channels:** Credentials shared in tools like Slack (e.g., Slack tokens) present vulnerabilities if the chat application is breached.

Severity Assessment:

- **Critical:** Credentials leaked in code repositories or used by third-party tools pose immediate risks.
- **High to Low:** Credentials stored within EC2 or shared across Slack channels are also high-risk but less immediately exploitable.

Mitigation Strategies

Mitigating Public IP Risks

1. Technical Solutions
   - **Automated IP Monitoring:** Develop scripts to periodically fetch and update public IPs, ensuring a current inventory.
   - **Public Exposure Flagging:** Flag any IPs associated with publicly exposed services and assess exposure risks.
   - **NMAP Scans on Public IPs:** Regularly perform scans to detect open ports and vulnerabilities.
   - **Automated IP List Refresh:** Configure the script to refresh IP lists automatically, keeping your monitoring up to date.

2. Process Improvements
   - **Approval Requirements for New IPs:** Require security team approval for all new public IP provisions to ensure each IP is justified and secure.

3. Enhanced Security Monitoring
   - **Request Logging:** Log each request to publicly accessible IPs to monitor for unusual access patterns.
   - **Web Application Firewall (WAF):** Implement a WAF to help mitigate attacks on exposed services.
   - **Rate Limiting and DoS Simulation:** Apply rate limits to public IPs and periodically simulate DoS attacks to test the effectiveness of rate limiting.

Mitigating Risks from User Credentials

1. Technical Solutions
   - **Multi-Factor Authentication (MFA):** Enforce MFA for all human users, making it significantly harder for attackers to exploit stolen credentials.
   - **Role-Based Access Control:** Avoid granting IAM or administrative privileges to service accounts, restricting elevated privileges only to human users with clear need.
   - **Credential Rotation:** Rotate IAM service account credentials every 90 days, minimizing the impact of compromised credentials.
   - **Vault Integration for Secret Management:** Use Vault or similar tools for securely managing and rotating credentials, reducing the risk of exposure.

2. Monitoring and Usage
   - **CloudTrail and SIEM Integration:** Enable CloudTrail logging and integrate it with a SIEM tool for real-time monitoring and alerting on anomalous activity.
   - **Activity Monitoring:** Continuously monitor IAM user activity to detect unusual usage patterns that may indicate compromised credentials.

3. Process Improvements
   - **Distinguishing Human and Automated Users:** Clearly separate human and automated user accounts to control permissions more effectively.
   - **Exit Notifications:** Notify IT, Security, and relevant teams when a user exits to prevent any orphaned access.
   - **OAuth-Only Tools:** Procure only tools that support OAuth to enhance security in third-party integrations.

Summary

1. **Primary Attack Vectors:** The most significant attack vectors in cloud environments are public IP addresses and user credentials, as they represent entry points that attackers can exploit directly.
2. **Mitigation through Review and Monitoring:** Regularly reviewing and securing public IPs, combined with robust credential management, can significantly reduce exposure risks.
3. **Layered Security for Credentials:** Keeping credentials updated, using tools like Vault, enforcing MFA, and integrating monitoring tools like CloudTrail create a layered defense strategy that strengthens cloud security.

By understanding and addressing these attack vectors, organizations can fortify their cloud environments against common threats. The cloud provides substantial flexibility and scalability, but with it comes the responsibility of vigilant, continuous security.

Security Cloud