Lateral Movement and Privilege Escalation Techniques

Lateral movement and privilege escalation are **common attack techniques where attackers navigate through a cloud environment to gain elevated permissions or access additional resources**. These techniques are especially critical in cloud environments due to the interconnected nature of services, identities, and APIs.

1. Lateral Movement Techniques

a. Using Cloud Service Accounts

- Definition: **Service accounts are non-human accounts used by applications or services to interact with cloud resources**.
- How They're Exploited
    - **Over-Permissioned Accounts**: Attackers use service accounts with excessive privileges to access resources.
    - **Token Hijacking**: Stealing API keys or OAuth tokens to impersonate a service account.
    - **Instance Metadata Exploitation**
        - Example (GCP): Extracting credentials from the metadata server via http://metadata.google.internal.
        - Command:

```
curl "http://metadata.google.internal/computeMetadata/v1/instance/service-
accounts/default/token" \
-H "Metadata-Flavor: Google"
```

b. IAM Role Switching

- Definition: Using one compromised account to **assume another role with higher privileges**.
- Example (AWS)
    - Exploiting **sts:AssumeRole** permissions to access other AWS accounts or services.

c. API Exploitation

- Definition: Leveraging **misconfigured APIs** to access or modify resources.
- Example
    - Exploiting API keys with unrestricted permissions.
    - Using cloud-specific CLIs (e.g., gcloud, aws-cli) to execute commands.

d. Exploiting Shared Storage

- Definition: Accessing **sensitive data stored in shared buckets, file shares, or blob storage**.
- Example
    - Misconfigured Google Cloud Storage (GCS) buckets with public access.

2. Privilege Escalation Techniques

a. Misconfigured IAM Policies

- How It Happens
  - **Weak IAM policies allow attackers to escalate privileges**, such as granting themselves additional permissions.
- Example (AWS)
  - Using an **over-permissioned IAM role** to attach policies to other roles.

b. Exploiting Default Credentials

- Example
  - Using **default or weak passwords for admin accounts** in managed services.

c. Exploiting Metadata Servers

- How It Happens
  - **Accessing sensitive credentials stored in instance metadata servers** (common in GCP, AWS, Azure).
- Example (Azure)
  - Extracting Azure Identity credentials via the metadata endpoint

```
curl "http://169.254.169.254/metadata/instance?api-version=2019-06-01" -H
"Metadata:true"
```

d. Code Injection in Functions/Serverless

- Definition: Modifying or injecting code into serverless functions (e.g., AWS Lambda, GCP Cloud Functions).
- Example
  - Attacker injects code into a GCP Cloud Function to access higher-privileged resources.

3. GCPloit Tool for Google Cloud Projects

What It Is

- **GCPloit is an open-source post-exploitation tool specifically for Google Cloud Platform (GCP)**.
- Purpose: Facilitates lateral movement and privilege escalation by exploiting misconfigurations and vulnerabilities in GCP environments.

Key Features

- **Enumerates IAM roles and permissions**.
- **Identifies over-permissioned accounts and exploitable resources**.
- **Automates privilege escalation techniques**.

Example Usage

1. Enumerate Permissions

- Lists IAM permissions of the current identity.

```
gploit list-iam
```

2. Privilege Escalation

- Attempts to escalate privileges using known techniques.

```
gploit escalate-privileges
```

3. Lateral Movement

- Identifies service accounts or APIs for moving across the environment.

```
gploit lateral-move
```

Use Cases

- Simulate attacks to test the security of GCP environments.
- Identify and mitigate misconfigurations.

4. Defense Strategies

a. Least Privilege

- **Restrict permissions** for users, roles, and service accounts to the minimum required.
- **Regularly audit** IAM roles and policies for over-permissions.

b. Secure API Keys and Tokens

- **Rotate API keys frequently** and **use environment variables or secrets managers to store them securely**.
- Enforce usage **restrictions on API keys** (e.g., IP whitelisting).

c. Monitor and Detect Abnormal Behavior

- Use tools like Google Cloud’s Cloud Logging and Security Command Center to monitor activity.
- Set up alerts for suspicious behavior, such as unexpected IAM role changes.

d. Metadata Server Protection

- **Block unauthorized access** to metadata servers using firewalls or proxies.
- Use Workload Identity Federation to limit access to sensitive tokens.

e. Implement Multi-Factor Authentication (MFA)

- **Enforce MFA** for all administrative accounts and access to sensitive resources.

f. Containerized and Isolated Environments

- **Use containerized environments** like Kubernetes to isolate workloads and restrict lateral movement.

5. Tools for Monitoring and Defense

Tool	Purpose
Google Cloud SCC	Monitors and detects misconfigurations in GCP.
AWS IAM Access Analyzer	Identifies overly permissive IAM policies.
Falco	Detects anomalous container activity in Kubernetes or Docker.
Azure Security Center	Provides recommendations for securing Azure environments.
GCPloit	Simulates post-exploitation techniques in Google Cloud Projects.

6. Summary

Technique	Description
Lateral Movement	Use service accounts, IAM role switching, API exploitation, or shared storage to move within a cloud environment.
Privilege Escalation	Exploit misconfigured IAM policies, metadata servers, or over-permissioned roles to gain elevated access.
Tool (GCPloit)	A post-exploitation tool to test GCP environments for lateral movement and privilege escalation paths.
Defensive Measures	Least privilege, secure API keys, metadata protection, and robust monitoring.

Lateral movement and privilege escalation are critical attack vectors in cloud environments. Tools like GCPloit demonstrate how attackers can exploit cloud services to achieve these goals. To mitigate these risks, organizations must enforce strict access controls, monitor for anomalies, and regularly audit their cloud configurations. Proper defense strategies ensure that cloud environments remain resilient to advanced threats.