CONTENTS

/01

云环境概述

云环境定义

将动态虚拟化的计算资源和应用程序，整合形成资源池，从而服务用户的平台或者互联网服务环境。

攻防视角下的云环境

云主机（ec2、ecs、cvm）
云数据库（rds、cdb）
云存储（s3、oss、cos）
云函数（lambda）
...

总结

云环境 = 身份 + 云服务集合。

云基础设施

容器逃逸
主机提权
网络隔离突破

云平台业务

AppSync跨租户访问漏洞
存储桶回源SSRF漏洞
日志敏感信息泄露漏洞

云租户业务

云凭据泄露
Web应用漏洞
服务组件漏洞

身份管理

创建和删除用户
用户属性配置
用户凭据

访问控制

策略定义与分配
RBAC

验证授权

MFA
临时访问票据

/02

云攻防技术剖析

云身份凭据泄露场景

前端泄露

- js文件
- apk安装包
- 小程序
- actuator heaphump

后端泄露

- 环境变量
- 配置文件
- ConfigMap
- 配置中心
- 硬编码代码

第三方泄露

- 代码托管平台
- 日志服务
- 云管理平台

元数据服务器

- SSRF
- IMDSv1
- IMDSv2

用户身份

aws iam get-user
aws sts get-caller-identity

用户权限

基于身份的策略：将托管策略和内联策略附加到 IAM 身份（用户、用户所属组或角色）。
基于身份的策略向身份授予权限。
托管策略
内联策略

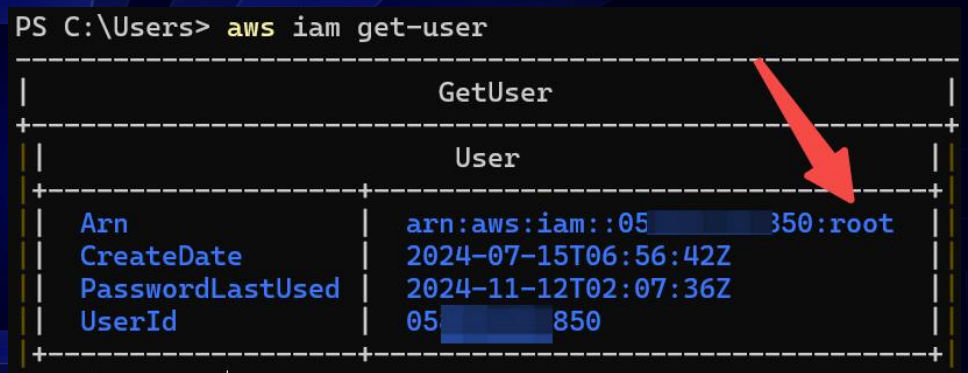
基于资源的策略：将内联策略附加到资源。

常用API

list-attached-user-policies
list-attached-group-policies
list-attached-role-policies
get-user-policy
get-group-policy
get-role-policy

根户权限

使用root账户凭据直接导致账号被接管，
控制租户所有云资源



用户/组管理

iam:CreateLoginProfile
iam:UpdateLoginProfile
iam:CreateAccessKey
iam:AddUserToGroup

攻击者通过用户/组管理API，将自身添加到特权组、修改特权用户登录密码、为特权用户创建永久凭据等方式提权。

```
{
    "Sid": "Statement1",
    "Effect": "Allow",
    "Action": [
        "iam:CreateAccessKey"
    ],
    "Resource": "*"
}
```

权限附加

iam:PutGroupPolicy
iam:PutRolePolicy
iam:PutUserPolicy
iam:AttachGroupPolicy
iam:AttachRolePolicy
iam:AttachUserPolicy

攻击者可以通过将包含高于其自身权限的策略附加到其用户、角色或用户所属的组来直接升级其权限

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "iam:AttachUserPolicy",
            "Resource": "arn:aws:iam::*:user/*"
        }
    ]
}
```

角色代入

iam:AssumeRole
角色信任关系

攻击者利用特权角色的过度信任关系实现权限提升甚至跨账户权限接管。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

运行在 EC2 实例上的应用程序可以通过特定的网址（http://169.254.169.254/latest/meta -data/）来访问元数据，元数据中存储EC2角色凭据。

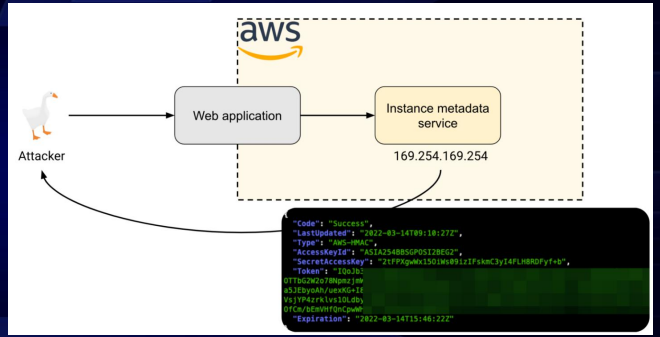
IMDSv1:

curl http://169.254.169.254/latest/meta-data/profile

IMDSv2:

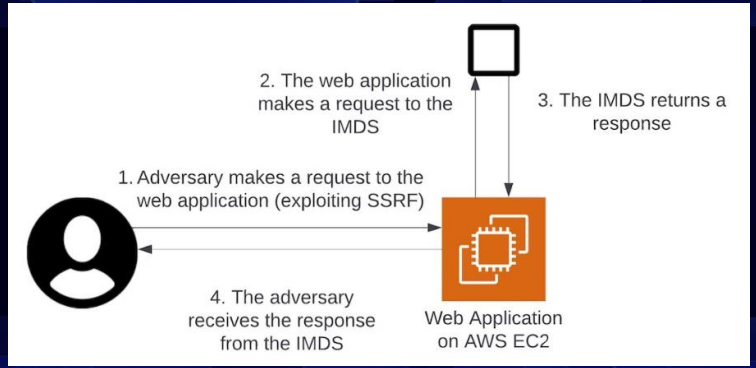
curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"

curl http://169.254.169.254/latest/meta-data/profile -H "X-aws-ec2-metadata-token: $TOKEN"



ssrf场景：

- 远程下载
- 在线阅读器
- http调试工具
- 回源配置



其他场景：

- 代理
- RCE

网络ACL过于宽泛
内网大范围扫描及横向移动
主机信息收集实现定向移动

VPC直通内网

可控云服务
业务信息收集
部署水坑
本地内网上线

VPC不通内网

- (IAM)创建后门账户
- (IAM)修改已有账户认证方式
- (IAM)滥用特权角色委派信任关系
- (EC2)user-data脚本执行
- (AMI)恶意镜像
- (Lambda)恶意代码注入

/03

云上攻防实战案例

前端代码中发现AK/SK

利用AK/SK在云主机中执行命令

在云主机业务系统中部署水坑，移动到目标内网。

初始访问

命令执行

横向移动


弱口令获取Jenkins后台权限
Jenkins所在EC2具有创建任意用户AccessKey角色权限
创建root用户AccessKey
初始访问
横向移动
权限提升

/04

云防御技术解析

云资产的发现与管理

漏洞探测

不安全配置管理

威胁监测和响应

cloudtrail

event hub

cloud audit logging

通过构建虚假身份信息或系统环境来吸引攻击者，使其暴露攻击意图、方法和来源

ADCONF

主场·见真章

THANKS