云渗透测试指南

CSA GCR cloud security alliance GREATER CHINA REGION ®

CSA cloud security alliance ®

云安全联盟顶级威胁研究工作组的永久和官方网址是：

https://cloudsecurityalliance.org/working-groups/top-threats/#_overview

序言

李克强总理在《2022 年政府工作报告》中指出 2022 年将强化网络安全、数据安全和个人信息保护，促进数字经济发展，加强数字中国建设整体布局。云计算已经成为企业数字化转型和数字经济发展的重要基础设施。

在当下日益复杂的网络环境中，评价公有云环境的安全性不能再采用单一的面向云基础设施的安全管控标准，为了充分识别云环境中的安全弱点和系统健壮性，对公有云上运行的系统和服务的渗透测试也成为保障云安全的重要技术手段。

此次发布的《云渗透测试指南》由 CSA 顶级威胁研究工作组专家编写，对当前全球化形势下针对公有云网络空间安全形势、安全风险的实质及特点，提出了应对的渗透测试方法和策略，并且对其中的要点进行了深入分析和阐述。

指南基于公有云场景已经达成广泛共识的共享责任模型，从云客户和云服务提供商两个视角对云渗透测试的范围（或边界）、测试目标、测试用例和关注点、合规性、测试相关培训和资源（如渗透测试工具）等进行了详尽地阐述。可以指导公有云客户系统全面地逐项评估其云应用、云服务的安全性。指南适用于从决策者到一线渗透测试人员的所有安全从业人员，尤其是云安全从业人员。可以让决策者充分理解云渗透测试的复杂性和重要性，同时为渗透测试人员提供了详尽的用例清单。

云是数字经济发展的基石，因此云安全在很大程度上将影响数据经济的发展。本指南是第一个云安全领域的渗透测试指南，相信它一定会为云渗透测试的发展起到引领的作用，同时为云安全乃至数字经济安全发展发挥应有的促进和推动作用。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

致谢

《云渗透测试指南》（Cloud Penetration Testing Playbook）由 CSA 顶级威胁研究工作组专家编写，CSA 大中华区秘书处组织翻译并审校。

中文版翻译专家组（排名不分先后）：

组 长：郭鹏程

翻译组：侯 俊 朱梦婷 薛 琨

审校组：郭鹏程 姚 凯

研究协调员：江瞿天

感谢以下单位对本文档的支持与贡献：

深圳市魔方安全科技有限公司 网宿科技股份有限公司

英文版本编写专家

主要作者：Alexander Getsin

贡献者：Asaf Hecht Michael Roza Jon-Michael Brook Shlomi Ohayon Chris Farris Greg Jensen Victor Chin

CSA 全球员工：Victor Chin

特别致谢：CSA顶级威胁研究工作组感谢 CyberInt 在本文档的开发过程中提供的支持。

在此感谢以上专家。如译文有不妥当之处，敬请读者联系CSA GCR秘书处给与雅正! 联系邮箱：research@c-csa.cn；国际云安全联盟CSA公众号。

目录

前言

安全测试是云环境、系统和服务实现安全保障的关键。在本文中，我们探讨在云环境渗透测试中最具主导性的安全测试模式。

根据NIST（美国国家标准与技术研究院）的定义，渗透测试是针对信息系统或独立系统模块执行专业性的技术评估，识别可能被对手利用的漏洞。这些测试能被用于识别漏洞或用于在一系列约束条件下，决定企业信息系统投入对抗的程度（如时间、资源和技能）[1]，ENISA（欧洲网络及信息安全局）针对渗透测试的定义与NIST[2]类似。

传统上，渗透测试的主要目标是识别技术上的安全弱点和系统健壮性。然而，安全测试更广泛地应用在评估企业的安全策略实现、合规要求的落实，员工安全意识的有效性，以及对安全事件的识别与响应能力。[3]因此，渗透测试对于任何全面的网络防御都是必选项，为系统安全提供可见性，并为系统和相关环境的安全提供高度可操作的缓解措施。

随着云服务持续在新技术领域的应用，大量商业组织大量将云作为基础设施。因此需要将渗透测试的范围扩展到公有云。

本文旨在为公有云渗透测试提供基础方法论，以及设计适用于公有云环境和服务的当前和未来技术的测试方法。此外，本文聚焦于对在云环境运行的应用和服务执行渗透测试，弥补了对公有云环境内的信息系统和应用程序进行安全测试的方法与认知差距。

目标受众

本文目标受众是渗透测试人员、云或基于云系统的安全从业人员。不过最初几页主要面向CIO、CISO和高级管理人员，帮助他们理解云端渗透测试的定义、范围、上下文、目标，以及如何在网络安全战略中落实。此外本文对开发人员和架构师设计云中系统的安全性也会有帮助。

本文目标：

- 提升读者对云渗透测试在网络安全战略中的重要性和云渗透测试方法的认识
- 为读者介绍云渗透测试的原则和注意事项
- 为渗透测试人员在公有云环境中更好地交付详尽全面的安全测试提供指导

[1] https://nvd.nist.gov/800-53/Rev4/control/CA-8#Rev4Statements
[2] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits
[3] https://www.fedramp.gov/assets/resources/documents/CSP_Penetration_Test_Guidance.pdf

本文范围

本文聚焦公有云环境上系统和服务的安全测试，即由云客户管理控制的系统与服务。例如，IaaS环境中云客户所管理与控制的虚拟主机就属于本文探讨范围，然而由云服务提供商控制的虚拟化管理程序（hypervisor）则不在本文范围内。另外对于混合云测试场景，混合接口和本地环境（内部部署，又叫遗留基础设施）也不在本文范围内。

本文涉及的云渗透测试方法与以下内容是互补的

- ***主题范围*** - 对如何测试云端应用和系统的部署/实现有指导，但不涉及应用程序本身的安全测试。那是 OWASP（开放Web应用程序安全项目）所覆盖的。
- ***现有测试和保障框架*** - 虽然其中概述了测试程序和交付阶段，以及一些并非云独有的测试用例，但这纯粹是为了上下文和尽职调查而做的，并不全面。云特有的测试用例和注意事项是对现有安全测试框架的有力补充，这样更简单也更方便与现有测试框架集成。

本文还提供关于公有云安全测试、培训机会和资源的范围界定，以及法律方面的思考与见解。

云渗透测试范围

基于云的系统、环境和服务的安全测试对于公有云来说是微妙且独特的。

共享责任模型的测试范围

由云服务提供商（CSP）全权负责的安全控制措施通常不在云用户委托的渗透测试范围内。例如，在软件即服务（SaaS）环境中，渗透测试人员被授权允许用特定用户的权限发起业务级攻击（即批准测试）。然而，测试人员不应在SaaS应用程序中测试访问控制（会话校验）或SaaS应用程序的输入过滤（即SQL注入）。这是因为测试会涉及破坏底层基础设施，超出了渗透测试人员所获得的权限范围。因此，除非获得CSP的明确许可，底层基础设施通常不在渗透测试的范围内。

云渗透测试不会挑战，而是考虑并利用底层技术的设计和代码完整性。例如：

- 在云服务、技术和服务提供中利用缺陷、常见错误配置和已知漏洞，属于基于云应用/资产测试的**范围之内**，但是针对云服务的取证、逆向工程和研究则**不是**。

共享责任模型

云渗透测试测的是云消费者权限范围内的安全性，而不是云本身的安全性。例如，在IaaS环境中，如图1所示，用户访问/身份、数据、应用程序和操作系统层都在范围内。而红线以下的所有其他组件，均由CSP控制和管理，因此不在范围内。同样的逻辑也适用于PaaS和SaaS环境的渗透测试范围，取决于云服务模型。

测试的程度和范围取决于云服务提供商提供的各种服务。尽管如此，云服务中意外发现的任何缺陷和漏洞也应给予通报。

蓝色 – 云用户/消费者安全责任

灰色 – 云服务提供商安全责任

图1. 共享安全责任模型

安全测试的范围和测试用例也因不同服务模型而异（图1）。在SaaS应用程序中范围较小：仅包括数据和用户访问/身份控制。在PaaS模式中，应用层（和一些平台配置）囊括在安全测试范围之内，所有较低的层都被排除在外。

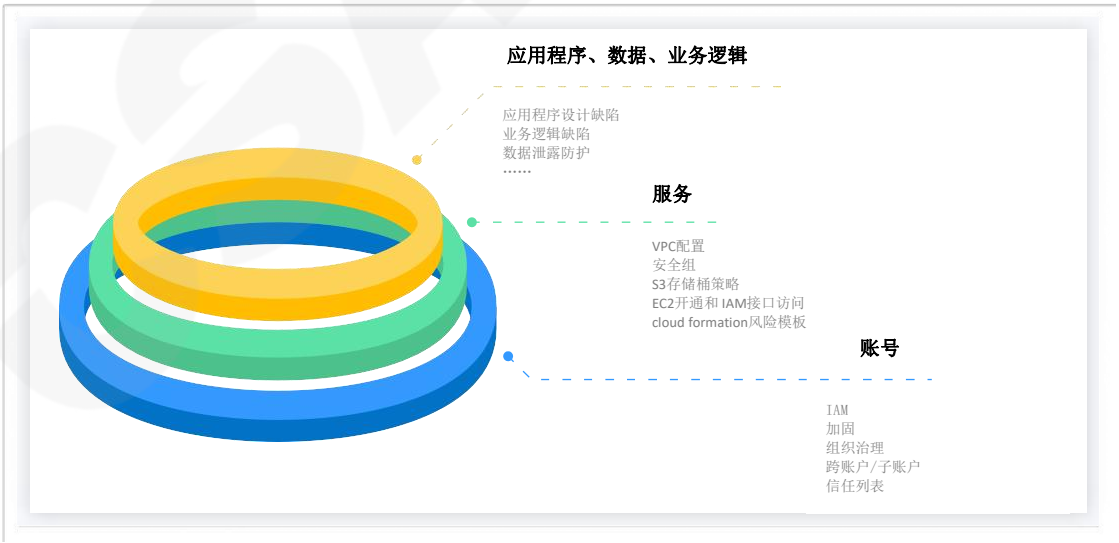
同样的原则也适用于IaaS，随着客户的责任边界扩大，潜在安全测试范围也会随之扩大。实施或移动工作负载都可能会改变潜在安全测试（和漏洞）的范围。会引入额外的测试范围（例如，云管理平面），但一些测试仍然由CSP负责（如虚拟化、硬件，有时还有操作系统）。

如果云客户从云服务提供商获得授权，在云服务提供商的控制和管理下测试云组件，那么云测试服务边界的划分将会变得更加复杂和模糊。

公有云渗透测试范围

虽然客户端应用程序在IaaS和PaaS环境的测试范围内，但本文并未详细介绍应用层（如SQL注入、XSS）和操作系统层（如虚拟机）测试方法，因为这些在OWASP和其他资料中均有详细介绍。因此，本文仅涉及以下方面：

- 与用户身份和权限相关的账户安全（如身份认证和鉴权、日志、账号加固、云身份联合和单点登录界面等）
- 与云租户可以配置的数据结构和云基础设施相关的云安全性（如S3存储桶策略、VPC网络访问控制、Cloud Formation风险模板等）
- 受终端用户控制的应用程序/业务逻辑安全（如应用程序设计缺陷、业务逻辑缺陷、代码脚本缺陷、数据泄露防护等）



即使其中任何一个被排除在渗透测试范围之外，渗透测试的范围也可以并且应该考虑这三个方面，因为这三个方面是互相影响的。

例如：

- 错误配置的用户账户（忽略了账户级的授权及访问控制机制）可能并将最终提高应用程序出现漏洞的可能性和漏洞的严重性
- AWS中的应用程序可能设计、应用或配置不当，导致其具备较高的云权限（例如拥有管理员权限），这被视为最高威胁。
- 忽视了账户级别的额度管控和预算控制可能会导致拒绝服务、资源不足或过度消费

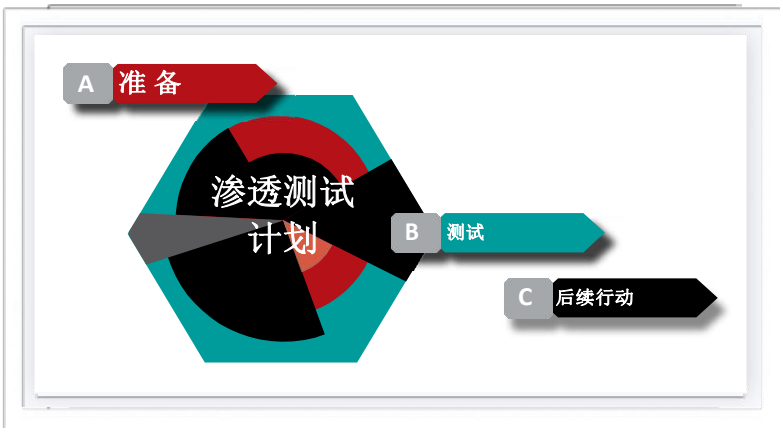
上下文中的云渗透测试

渗透测试，也称动态测试，通常在代码开发和部署后运行，即便不在生产环境中。重要的是要记住，渗透测试不一定是最好或最有效的测试形式，它的适用性取决于需求背景和目的。例如，当评估对象是部署在云环境中的活跃产品或功能时，建议采用本文所述的方法测试，但若只是为了评估某一个刚刚被设计的功能，威胁建模是最佳选择。

在微软定义的安全开发生命周期中，安全测试工作处于验证阶段，包括动态测试和威胁模型/攻击面验证。

保障计划

渗透测试也可以（并且经常）成为安全计划的一部分， CREST 一直在倡导他们的测试计划。



CREST的计划旨在帮助组织有效管理正在执行或交付的渗透测试，概述了将渗透测试的价值最大化的步骤以及最佳实践，因此看起来似乎存在一些“重复的范围”，但必须指出的是，渗透测试服务接收者的**“准备期”**是有别于渗透测试提供者（即提供渗透测试服务的厂商）的“准备期”的。本文中描述的方法是从安全服务提供商的角度写的，这种角度符合并满足一些“客户/接收者”的需求，例如在**测试阶段**，特别是“使用有效的测试方法”的需求。

“后续行动”阶段为渗透测试的接收者提供了指导，指导他们根据交付的成果采取行动，以及评估渗透测试的有效性，这不在本文档描述的范围内。另外，如果云环境/系统在范围内，那么本指南会做出说明，非云范围的还是需要各自的方法和参考。

云渗透测试指南改编自CREST测试方案的准备（第3部分）和测试（第4部分）两个章节，并提出了5个主要阶段：准备、威胁建模、侦察和研究、测试以及报告撰写。本文档详细介绍了每个阶段中独特的云安全测试用例和注意事项。

云渗透测试的目标

渗透测试的目的是识别代码漏洞、配置漏洞以及其他不安全的实现，并给出有效的缓解建议。

请务必记住，以下测试用例仅仅考虑独特的、云场景下的测试用例和缺陷。云只是承载了许多不同功能和用途（例如工作负载、存储或容器）的画布，渗透测试的结果因云上部署的业务而异，正常来说，这些组件需要参考自己的测试指南。

我们选择模型是**STRIDE**，它是微软为识别计算机威胁而开发的威胁模型，通过探索可能出现的错误指导攻防工作。我们通过STRIDE模型对建议的测试用例分组，因为它的术语和格式已经被广泛认识和使用。

- **欺骗** - 冒充、伪装或以其他方式伪造自己的身份或特征。在云渗透中，身份欺骗通常采用窃取云环境登录凭据的的方式去利用该账号的权限。
- **篡改** - 破坏、修改或伪造记录、进程或产品，达到恶意的目的或为攻击者的其他目标或攻击链服务。在云测试中，篡改通常采取修改日志记录、修改主机镜像、篡改API、数据库或数据的形式。

- **抵赖** - 造成对日志或数据的真实性存在争议、缺乏或损害的情况。云测试中的抵赖通常采用删除或关闭日志记录的方式，或利用云服务和机制来掩盖某个行为或事件。
- **信息泄漏** - 隐私侵犯或向未经授权的对象或公众泄露信息。在云测试中，信息通常从错误配置的公有云存储中泄露。
- **拒绝服务** - 使目标用户无法使用系统、功能或资源的行为。在云测试中，拒绝服务通常采取破坏或加密云资源、禁用账户、凭据或用户的形式出现。
- **权限提升** - 利用漏洞或配置实现超出预期的访问权限或特权提升的行为。在云测试中，权限提升通常采取利用错误配置的IAM权限的形式，这些权限允许升级，或允许使用受损服务或目标系统。

云渗透测试用例和关注点

黑色的项目是已经包含在标准渗透测试任务和框架中的传统项目。蓝色的项目与云环境相关，应该考虑予以测试。通常情况括号里的内容是示例或参考。

1.准备工作

a.与用户签订保密责任和测试协议

b.定义并同意渗透测试的目的和范围

i.确定测试限制条件

ii.确定作用范围内的目标和环境

1.云账户是否在范围内?

2.云供应链服务和合作伙伴是否在范围内？

3.在范围内是否考虑了不同的租户?他们被排除在外了吗? 他们目标明确吗？什么被认为是独立租户？

4.是否考虑获得 CSP 测试的批准/限制？

5.了解对公有云的攻击量和风险的详细评估

c.依据适当的（通常是公开的）安全测试过程，对每个云服务提供商和用户进行云渗透测试

d.提供、接收需求规范

i.考虑云合规、指导和框架（例如 CSA CCM）

e.制定、同意并签署渗透测试工具、策略和程序（TTP），以及方法论

i.非云 TTP，如 OWASP 应用程序测试指南

ii.云侦察，网络钓鱼，账号劫持/密码重置 TTP

iii.用于识别漏洞利用的云审计最佳工具 Azurite, ScoutSuite

iv.用于欺骗、篡改、拒绝、信息泄露、拒绝服务和提高特权的可接受的和最低限度的测试用例

v.对目标、结构和证据采取行动，以证明测试成功并达到目标

vi.实施管理控制和操作流程

vii.指定联络点

viii.提交和管理变更请求

ix.解决测试操作问题

x.隔离、限制和解决测试对系统的影响

2.威胁模型

a.将用户的关注点、目的和各种规范都包含在威胁模型中

b.在范围内执行威胁模型

i.通盘考量特定云服务提供商，部署和使用威胁模型

ii.考虑云威胁（最大威胁）的行业标准/云威胁最佳实践

1.12项云计算安全威胁，网络攻击树

3.侦察和研究

a.进行标准侦察（记录、网站、网络、IP 指纹、犯罪记录、人、社交媒体）

i.利用DNS 记录 （N, MX, NS, SPF, TXT, CName, A）确定目标域或企业中可能的管理不当或被劫持的云提供商和服务

ii.通过谷歌接口和DNS记录的adfs, auth, fs, okta, ping, sso, sts, oauth, openID, saml, ws，对技术和服务提供商等身份联合服务器侦察

iii.在代码和文本存储库中查找云凭证（如API密钥、联合身份服务私有证书和存储账户密钥/sas、亚马逊公开设置文件证书）

iv.从受损的凭证转储中或通过OSINT，收集和穷举云用户和管理凭据

v.通过领英、公司网站识别云管理、运营、用户和供应链人员目标

vi.通过证书透明日志和DNS记录（company bucket.s3.amazonaws.com）识别云服务、资产和域名服务器记录

vii.识别范围和相关的云存储实例、账户和服务

viii.查找云账户和系统的介绍、设置和配置文件（例如亚马逊公开设置文件，app.config or aws/azure .config files）

ix.通过服务API调用枚举账户、用户和/或角色（通过服务 API 调用枚举账户、用户和/或角色（例如使用账户内已知或公共资源标识符的 AWS 枚举，或盲目地使用 UpdateAssumeRolePolicy）

x.进行漏洞利用环境/账户侦察，以确定账户id、别名、账户组织结构和云模型、受损用户IAM、以及其他用户

xi.识别不同的云模型账号（例如亚马逊公有云与政务云），不同的账号类型（如Azure ARM、Azure ASM账户、Azure存储账户）

xii.分析移动应用程序和本地应用程序的云服务/账户秘密、用户、角色、资源名称（arn、AWS密钥、Azure存储账户名称、AWS存储桶名称）

xiii.侦察开发后环境、账户，确定高价值系统、资产和用户

b.研究

i.已识别的资产侦察

1.已知漏洞

2.常见错误配置

3.开发工具和方法

4.审查云技术和云服务提供商的安全公告；它们可能会产生未修补损害向量（AWS Bulletin）

ii.将侦察结果纳入威胁模型

4.测试

a.验证基线安全需求

b.采用与控制域和技术相关的安全测试用例、指南和清单

- web？移动端？本地？服务器端？API？
- c# mvc? objective c IOS? Python redhat? c++ winforms

c. 用户身份和其他实体的欺骗测试

i.窃取硬编码的无服务器工作负载函数（作为函数实现的工作负载）凭据和秘密（比如硬编码的Azure函数代码，或者拉取lambda部署包）

ii.通过云服务配置或负载均衡器实例尝试负载均衡MiTM漏洞会话劫持（elb弹性负载均衡）尝试把域名转移到另一个禁止转让域名的注册商（Route53，又名域名劫持）

iii.窃取环境变量和本地文件凭据，以利用和模拟用户标识（例如AWS、实例元数据、shell变量、azure ServiceBusExplorer.exe实用工具、配置文件、ecs任务定义或azure ARM配置令牌）

iv.从代理或http转发服务器的元数据中窃取凭据（AWS元数据中的证书）

v.窃取云工作负载凭证（AWS元数据sts或Azure Linux 代理 （waagent）文件夹凭证）

vi.在遗留云环境和服务中承诺默认的特权服务和用户账户（比如Azure中以前的ASM共同管理员账户或Azure存储账户密钥）

vii.窃取云控制台或服务器证书（比如Azure asm证书）

viii.窃取云唯一凭据（如AWS sts临时服务令牌或azure SAS令牌）

ix.通过云密钥服务或利用特权进行操作来窃取凭据（aws 密钥管理服务, azure 关键

库）

x. 形成针对云用户、管理员和供应链人员及公司的鱼叉式网络钓鱼

xii.利用受损或配置错误的云电子邮件服务进行商业电子邮件侵害和进一步的网络钓鱼（例如，如果SES被配置为允许从@company.com发送邮件，那么SES:*的身份管理权限可以发送一个看起来来自内部的SES电子邮件）

xiii.窃取cookie，秘密，口令，kerberos票据，身份令牌

d.篡改测试

i.更改数据存储中的数据，防止进行欺诈性交易或静态网站侵害（s3, rds, redshift）

ii. 更改无服务器函数、逻辑应用程序或其他业务逻辑，以实现目标或升级权限（AWS lambda或Azure logic apps）

iii.更改计费阈值和警报（AWS费用,篡改自定义阈值和cloud watch警报）

iv.更改应用程序、网站或其他代码完整性，导致资源滥用、持久化、外泄或其他问题（AWS s3静态网站或Azure网站）

v.在受信任区域和/或证书中创建或更改DNS记录集，以分流流量、创建网络钓鱼网站，滥用品牌（AWS ACM, AWS Route53, Azure DNS服务）

vi.更改本地sql或mysql数据库中的数据

e.抵赖测试

i.在未启用日志记录或禁用全局日志记录的区域进行操作（如CloudTrail）

ii.更改未经验证的日志存储区中的日志文件或禁用验证（如cloud trail日志验证）

iii.禁用网络流量分析/日志记录（VPC flowlogs）

iv.禁用云警报，防止检测和响应（比如cloud watch警报、GuardDuty、Security Hub或Azure安全中心）

v.禁用数据存储访问日志，以防止检测和响应（Cloudtrain数据访问，s3访问日志，redshift用户活动）

vi.更改日志的保留情况或损坏日志的完整性（s3生命周期、kms解密、cmk密钥删除、

角色特权锁定）

vii.更改本地Windows/Linux系统日志

f.信息泄漏测试（隐私泄露或数据泄露）

i.利用错误配置和默认的安全组和访问列表，将数据泄露到任意互联网IP地址（vpc acl, instance sgs）

ii.尝试使用服务端点和mitm进行数据库缓存和内存缓存数据泄漏（弹性缓存）

iii.创建新的大数据任务，处理敏感数据并将其输出到可访问的数据存储（emr, s3）

iv.从具有cli /转储的可公开访问的数据存储服务s3, rds, rds快照, redshif集群, elastic search 域）或私有存储（s3 aws cli get, dynamodump）中收集数据，相应地对它们进行配置以进行外泄

v.利用云邮件和短信分发服务窃取数据（ses, sns）

vi.访问配置错误的消息队列，以访问可能处于队列中的敏感数据（AWS SQS）

vii.窃取和利用虚拟机元数据（例如VPC专有网络、子网、账号、身份管理角色、角色证书）

viii.从代理或http转发服务器的元数据中窃取元信息（AWS元服务器中的证书）

ix.从存储账户中窃取虚拟机镜像和快照；分析它们的敏感数据（例如存储账户中Azure虚机磁盘快照，公共或专有的AWS EBS快照和AMIs）

x. 指纹服务器、应用程序版本、框架，检测应用程序日志中的敏感个人身份识别信息

xi.尝试使用MiTM窃取数据

g.拒绝服务测试（DoS）

i.销毁/加密数据存储中未备份的数据，或破坏保护（s3、rds）

ii.通过从云环境中大量发送电子邮件或SMS消息，拒绝服务或服务器和客户端的可操作性（AWS sns, ses）

iii.破坏云服务配置、数据存储、账户（使用——dry- run AWS cli标志或证明您有权限）

iv.通过删除可以访问KMS密钥的所有身份识别用户或角色，拒绝访问该密钥

v.对应用程序执行基于容量的拒绝服务攻击或应用程序拒绝服务攻击，按照CSP和用户政策以及协议，做到极尽全力的告警

h.提权测试

i.使用更高权限触发云编排自动化（例如具有高度特权角色的云形成堆栈)

ii.使用分配/传递的服务或角色运行或部署工作负载，导出这些特权的实例凭证（例如ec2传递的角色和元凭证）

iii.利用策略写功能更改或创建分配给用户的不受限制的策略（例如:CreatePolicyVersion）

iv.更改用户或新用户的默认策略，以包含额外的特权 （例如 set- default-policy-version）

v.创建或重置属于高权限用户的登录、访问密钥或临时凭据 （例如 iam:CreateAccessKey, sts or iam:UpdateLoginProfile）

vi.将策略添加或更新到有权访问的角色、组或资产（例如 iam:AttachGroupPolicy, iam:PutUserPolicy, sts:AssumeRole）

vii.利用开发者和替代控制台来代表他们执行特权 （AWS Glue Console endpoint with pass role, Azure machine learning studio）

viii.利用数据或代码管道代表假定的角色执行操作 （AWS data pipeline ShellCommandActivity, inject python code into a pickle celery sqs queue）

ix.传递角色并为虚拟机分配高实例特权，然后可以对虚拟机进行控制，并将其用于AWS API调用（例如create-instance-profile 和 iam:passrole）

x.使用描述性特权窃取应用程序或代码管理凭证（例如 Get- AzureWebsite -Name webappname）

xi.导出服务和其他账户类型密钥（例如Azure Get-AzureStorageKey-StorageAccountName “Storage_Account_Name”）

xii.向现有角色或组中添加具有更高权限的用户、资产或账户（利用

iam:AddUserToGroup等权限）

xiii.进程hooking，进程注入，windows访问令牌操纵，利用错误配置的sudo功能

i.**其他测试用例和目标**（非微软威胁模型的横向移动测试用例）

i.横向移动

ii.利用错误配置的安全组和访问列表在云中的资产（EC2、RDS和其他）之间横向移动，从一个账户到另一个账户（AWS跨账户承担角色）

iii.在受损机器上的目标网络/子网中创建一个额外的接口/分配和IP地址（比如为AWS ec2分配一个次要的私有IPv4地址或接口）

iv.创建定时任务或无服务器操作，向机器和用户添加根证书和ssh私钥（如AWS lambda）

v.从存储账户窃取虚拟机镜像，分析它们的密码，密钥和证书来访问活跃系统（像azure vm vhd快照从存储账户）

vi.通过工作负载管理服务权限（AWS SSM或Azure Agent）获得对实例/ vm的操作系统级访问权限

vii.利用本地网络系统上的应用程序和服务; 利用文件共享、脚本框架（如powershell）、操作系统编排（如WMI）和管理框架（如配置管理器）

j.持久性

i.给内部资源分配一个公共IP（AWS cli / console -弹性IP）

ii.建立一个备选的云本地/服务控制接口（如AWS Glue控制台、工作区或Azure脚本/串行控制台）

iii.配置账号/用户恢复的详细信息，包括备份联系人（如AWS替代联系人）

iv.编辑自定义机器镜像和模板，以包含持久性机制（如AWS自定义ami中的反向shell）

v.创建跨云服务提供商，跨账户的持久连通性（例如VPC终端，允许自己账户的所有流量进入内部网络，使用安全的账户）

vi.通过配置好的负载均衡器发布内部资源（如ssh, rdp或80通过ELB负载均衡器）

vii.使用工作负载/警报发现故障及时通知，以维护持久性（AWS lambda函数，cloudwatch, ec2）

viii.具有管理权限的可调用函数和或API，调用它来获取API Key/Secret/Token（如AWS lambda & API网关）

ix.使用特权事件源驱动的工作负载作为后门、shell或持久化机制（lambda向安全组添加规则、向用户添加密钥、监听日志、ec2、elb或其他事件以管道shell命令、从internet上触发SQS命令事件）

x.创建系统管理命令或滥用实例元数据来调度和触发命令和控制（AWS系统管理器，修改EC2 UserData来触发一个反向shell）

xi.使用云本地系统管理工具（aws系统管理）执行远程代码

xii.为虚拟机实现一个启动脚本（比如Azure启动脚本）

xiii.向现有用户和服务添加凭据（例如AWS安全凭据访问密钥）

xiv.创建具有模糊但可升级特权的影子管理用户或角色（如AWS CreatePolicyVersion和SetDefaultPolicyVersion特权）

xv.创建具有远程控制权限的本地实例用户（ssh/rdp）

5.报告

a.报告的关键点

i.参考行业标准和云安最佳实践/配置（云安全联盟CCM，AWS良好架构框架）

ii.收集和报告云账户、别名、元数据、密钥和amis的证据

b.后续工作

i.Crest 跟踪阶段事项，如监控计划的实施和测试效果的评估

法规

渗透测试需要遵守所有适用的地方和国家法律。在提供任何渗透测试服务之前，应获得正式的书面和签署的客户授权。

测试人员和客户还应该考虑任何合法的供应链要求。属于测试范围的第三方供应商和服务可能有自己的检测指南、程序、限制和要求。例如,

- AWS不再强制要求颁发测试许可。但是，这里仍然有几个限制条件。
- 可能影响欧洲公民个人身份信息（PII）的测试必须考虑，任何此类数据都必须按照GDPR指南进行处理（匿名化、传输中的安全处理、违规报告）。 这一点可能经常被忽视，因为GDPR首先要求进行此类测试。

培训和资源

培训

我们推荐研究CSA的《云计算关键领域安全指南》。此外，以下资源可能也很有用。

实验室 & 资源

除了设置你自己动手实践或工作经验之外，很少有攻防类的云安全实践培训机会；然而，以下是可取的:

- FLAWS -通过一系列有关使用AWS时常见错误和“陷阱”的关卡，以闯关的方式学习
- CloudGoat Rhino-安全实验室的“设计缺陷”是AWS基础设施设置工具

工具

有许多用于评估和测试云环境及其内部安全性的开放工具可用，主要包括：

- NCC Groups开源云审计工具（ScoutSuite等）-一个多云审计套件
- LazyS3 - 枚举 AWS s3 的工具
- CloudBurst - 一组工具，包括（Azure）服务枚举、数据存储、凭证收集等
- Nimbusland - 一个解析云IP地址空间的工具
- pacu - 一个AWS 漏洞利用工具包
- Shodan - 该搜索引擎可以帮助识别、研究和侦察基于云计算的公共系统和资产

一个更全面的开放云安全工具可以在ToniBlyx上注册。

结论

自十几年前云计算概念提出以来，云已经从一个受到许多批评和质疑的新技术范式变成了一种被广泛接受的信息技术形式。虽然云计算的使用已经规范化，但安全最佳实践和流程仍然需要不断更新、开发和完善，以确保成功。本文为公有云环境中的系统渗透测试提供指导。渗透测试人员将能够参照本文的测试目标测试公有云系统和环境的安全性。本文还讨论了法律和其他相关问题，通过对关键决策者的培训，使他们了解云渗透测试的复杂性。CSA顶级威胁工作组希望您就这些关键问题提供建议，这将使云渗透测试更加成熟，也将有利于创造更安全的云计算环境。

参考

1. https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf
2. https://www.owasp.org/index.php/OWASP_Testing_Guide_v3_Table_of_Contents
3. Penetration Testing Execution Standard （PTES）
4. http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html
5. https://www.youtube.com/watch?v=ge6gJkb3nXE A Penetration Tester's Guide to the AzureCloud
6. https://labs.mwrinfosecurity.com/assets/BlogFiles/mwri-a-penetration-testers-guide-to-the- azure-cloud-v1.2.pdf
7. https://vimeo.com/214855977
8. Gone in 60 miliseconds aws
9. https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/
10. https://github.com/dagrz/aws_pwn/blob/master/miscellanea/Kiwicon%202016%20-%20Hack- ing%20AWS%20End%20to%20End.pdf
11. Daniel Grzelak AWS Account Backdoor, Daniel Grzelak AWS account post compromise
12. https://medium.com/@cloud_haxor/enumerate-aws-account-ids-and-iam-resources-c374843cfdf4
13. DEF CON 25 - Gerald Steere, Sean Metcalf - Hacking the Cloud
14. https://www.cyberark.com/threat-research-blog/cloud-shadow-admin-threat-10-permissions- protect/
15. https://gbhackers.com/cloud-computing-penetration-testing-checklist-important-considerations/
16. https://www.cloudconformity.com/conformity-rules/
17. https://attack.mitre.org/wiki/Lateral_Movement

18. https://www.blackhat.com/docs/us-16/materials/us-16-Amiga-Account-Jumping-Post-Infection- Persistency-And-Lateral-Movement-In-AWS-wp.pdf

19. http://www.chrisfarris.com/post/lateral-movement-aws/

20. BSidesSLC 2017 -- Bryce Kunz -- Pwned Cloud Society

21. Blue Cloud of Death - Red Teaming Azure

22. https://www.microsoft.com/en-us/securityengineering/sdl/howto

23. AWS ELB neglecting internal server TLS certificates

24. http://www.irongeek.com/i.php?page=videos/derbycon8/track-3-16-cloud-forensics-putting-the- bits-back-together-brandon-sherman-