安全十

EISS-2020
企业信息安全峰会
之北京站

2020.07.31

云上攻防

王任飞

安全小飞侠(avfisher)

01

个人介绍

whoami

- 王任飞 (avfisher)
- 公众号“安全小飞侠”作者
- 专注于红蓝对抗、漏洞研究、安全架构、云安全等领域
- 曾负责某国际TOP3互联网公司的中国区的Blue & Red Team，现任某公有云厂商蓝军团队负责人。

02

Red Team介绍

定义

Red Team的概念最早来源于20世纪60年年代的美国军方方，指的是一一个通过承担对抗性角角色色来挑战组织以 提高高其有效性的独立立的团体叫做Red Team。

类型

- 模拟直接威胁者：根据特定的威胁情报来模拟攻击者，所谓“以情报驱动的Red Teaming行动”，目前深受国际主流互联网企业的Red Team团队的青睐，例如针对某些特定行业或者国家的APT组织的TTPs的模拟

- 模拟已知威胁者：根据已披露的APT组织的TTPs来模拟攻击者，例如利用ATT&CK来规划和映射Red Teaming行动所需的TTPs

- 模拟未知威胁者：根据真实入侵的各个阶段收集到的具体目标信息实时地规划攻击路径从而模拟攻击者

03

Red Team建设

方法论

- 目标范围：场景化的具体的行动目标（如窃取客户财务数据，访问CEO的邮件，控制云服务管理服务器，控制云上租户的云资源等），攻击范围，授权许可，行动时间，行动约束（Rules of Engagement）

- 情资搜集：威胁情报（0day漏洞研究与Nday漏洞利用、最新攻击手法等）和目标资产（IP、域名、员工信息、初始入口等）的收集

- 行动计划：攻击计划与TTPs准备

- 行动执行：实施攻击

- 记录报告：文档记录，行动报告

行动流程

攻击计划

- 行动准则（授权与禁止行为，授权范围，限制条款等）
- 风险管理（提前识别和管理行动过程中的各种潜在风险）
- 行动计划（威胁情报，ATT&CK TTPs等）
- 报备与授权流程
- 行动终止流程
- 行动成本与预算

攻击执行

- 备案的时间区间内
- 备案的目标范围内
- 备案的攻击IP与网络环境

攻击完成

- 恢复所有修改
- 移除所有payload和backdoor
- 移除所有持久化控制
- 关闭所有C2通道
- 提交攻击报告与改进建议（执行总结，方法论与目标，攻击场景与范围，攻击过程与时间线，关键发现与改进建议）
- 开始复盘会议（技术层面）

运营管理

行为管理

- 权限管理
- 政策控制
- 物理控制
- 软件控制
- 内部共享资料库管理

数据管理

- 事前情资数据
- 攻击行为记录
- 操作日志
- 自动化数据收集与日志
- 攻击行为截图
- 事后攻击数据（攻击报告，数据归档，内部报告分发等）

04

云上攻防实践

云上攻击类型

- 利用公有云上租户的不安全的应用与服务配置为突破口

- 利用公有云本身的服务（IaaS，PaaS，SaaS）的自身问题为突破口

云上租户为突破口

场景一：云服务认证Key泄漏（如AWS AK/SK或者Security Token等）

- 攻击难度：低
- 攻击路径：云服务认证Key -> 云服务公开API/SDK -> 云服务资源访问/控制
- 利用方式：
  - ☑ Github仓库配置不当
  - ☑ 云架构中的密码重用
  - ☑ 针对云租户账号密码的社工攻击（如AWS Credential Harvesting钓鱼攻击）
  - ☑ 云主机中Web应用的漏洞（SSRF，RCE，本地文件读取等漏洞）
  - ☑ 公共的存储桶
  - ☑ 信任的关联第三方数据泄露
  - ☑ 硬编码在网页或移动APP中的AK/SK。
- 相关参考：
  - AWS MFA Phishing: https://rhinosecuritylabs.com/aws/aws-phished-persistent-cookies/
  - AWS IAM Keys: https://rhinosecuritylabs.com/cloud-security/onelogin-breach-cloud-security-and-protecting-aws-ami-keys/

云上租户为突破口

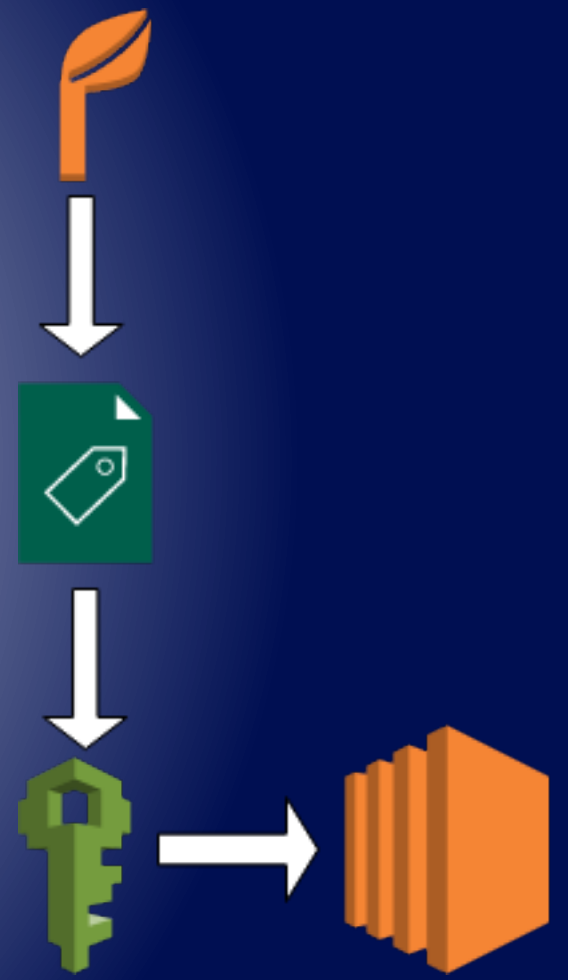
场景二：云上租户的云服务不安全配置

- 攻击难度：低
- 攻击路径：公共访问的云存储桶 -> 敏感凭证 -> 云服务资源访问/控制
- 利用方式：公共访问的云存储桶爆破
- 相关参考：
  - GCP: https://github.com/RhinoSecurityLabs/GCPBucketBrute
  - AWS:https://github.com/RhinoSecurityLabs/Cloud-Security-Research/tree/master/AWS/s3_bucket_bruteforcer

云上租户为突破口

场景三：云主机中web应用自身漏洞

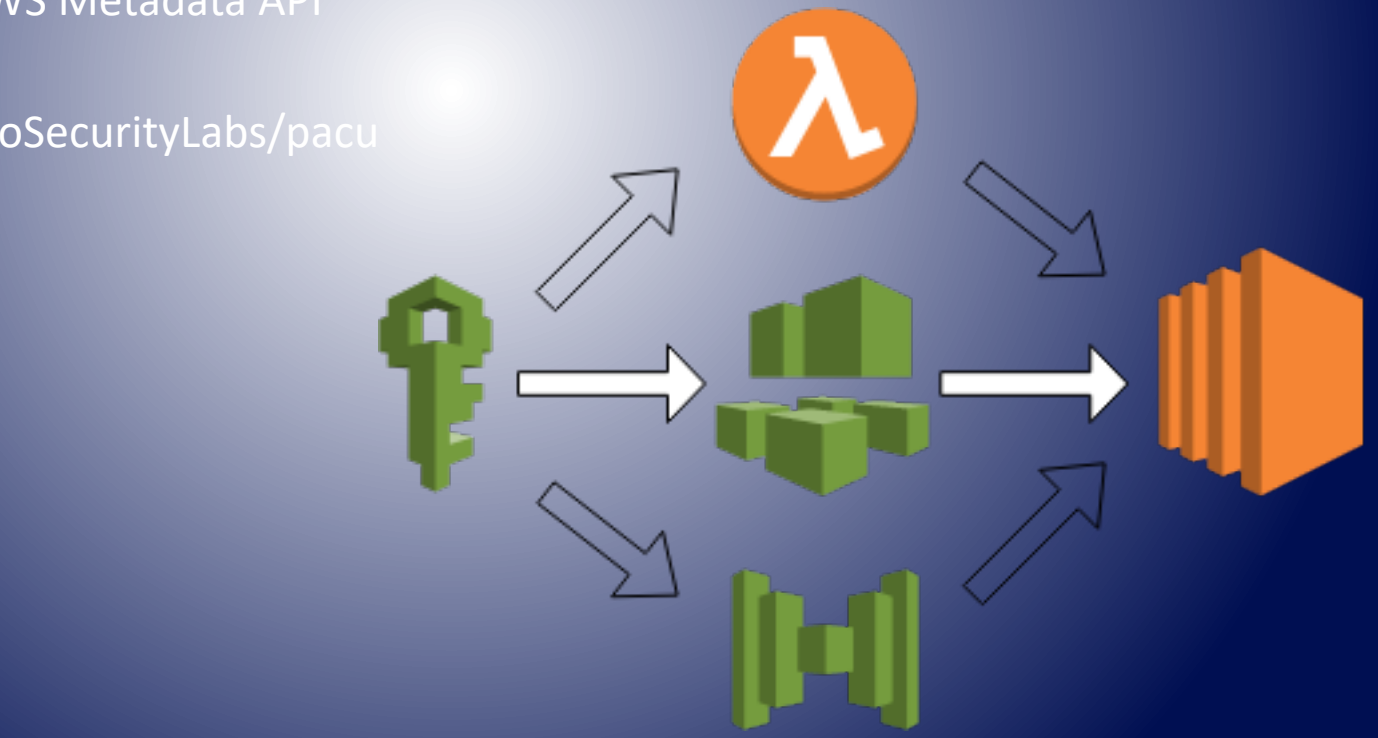
- 攻击难度：中
- 攻击路径：
  - SSRF -> EC2 Metadata API -> IAM临时Security Token -> AWS SSM -> RCE
  - SSRF -> EC2 Metadata API -> IAM临时Security Token -> AWS Lambda -> RCE
  - SSRF -> EC2 Metadata API -> IAM临时Security Token -> AWS S3 -> 信息泄漏
  - RCE -> EC2 Metadata API -> IAM临时Security Token -> AWS EC2/S3/Lambda
  - RCE -> EC2 Metadata API -> EC2 Userdata -> 敏感凭证 -> 其他EC2或者云服务
- 利用方式：Web应用漏洞（如SSRF/XXE/RCE等）
- 相关参考：
  - AWS Elastic Beanstalk: https://www.notsosecure.com/exploiting-ssrf-in-aws-elastic-beanstalk/
  - AWS SSM: https://hackerone.com/reports/401136
  - AWS:https://blog.appsecco.com/getting-shell-and-data-access-in-aws-by-chaining-vulnerabilities-7630fa57c7ed
  - CloudGoat(AWS):https://rhinosecuritylabs.com/aws/cloudgoat-walkthrough-rce_web_app/
  - GCP: https://hackerone.com/reports/341876



云自身为突破口

场景一：云服务自身功能导致代码执行

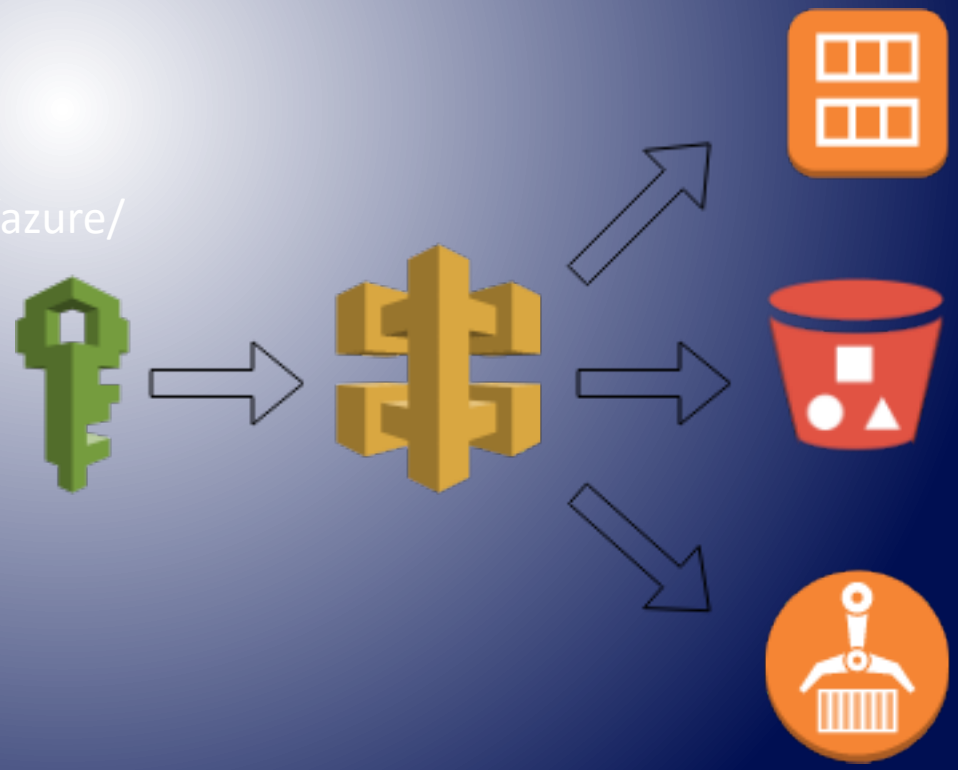
- 攻击难度：低
- 攻击路径：云服务账号AK/SK -> 云服务功能（AWS SSM/Lambda/EC2 Instance Connect） -> RCE
- 利用方式：
  - ☑外部泄漏的云服务账号AK/SK（Github，Public S3 Buckets，硬编码在网页或移动APP中的AK/SK等）
  - ☑EC2云上应用SSRF漏洞配合AWS Metadata API
- 相关参考：
  - AWS: https://github.com/RhinoSecurityLabs/pacu



云自身为突破口

场景二：云服务的公开API利用

- 攻击难度：低
- 攻击路径：云服务账号AK/SK -> 云服务公开API -> 云服务资源调用（OS镜像，容器镜像，存储桶，数据库，Userdata等）-> 敏感信息泄露（数据，凭据等）
- 利用方式：云服务公开API的熟悉和利用，如AWS CLI/AWS SDK
- 相关参考：
  - AWS: https://docs.aws.amazon.com/
  - GCP: https://cloud.google.com/apis
  - Azure: https://docs.microsoft.com/en-us/rest/api/azure/



云自身为突破口

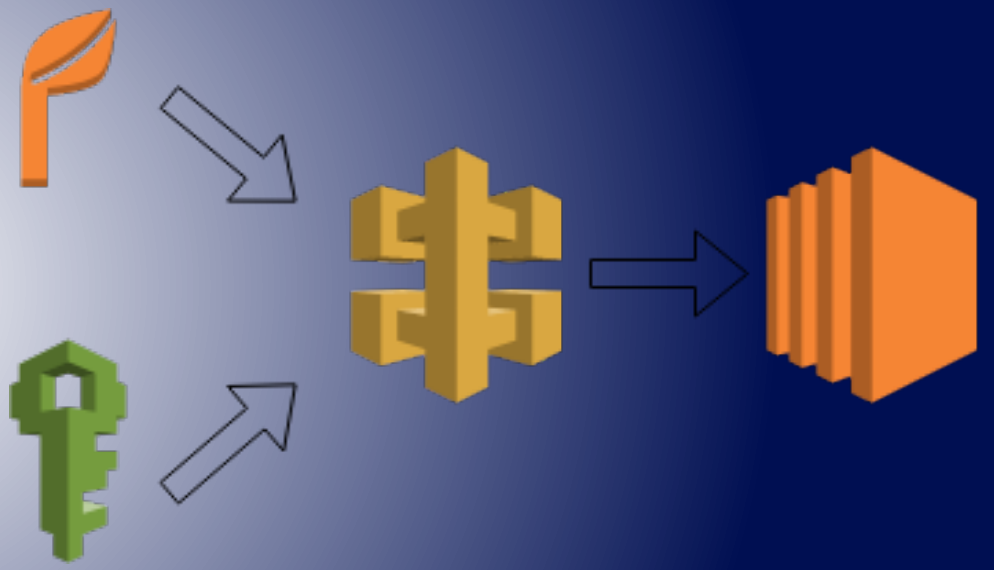
场景三：云服务第三方软件漏洞利用

- 攻击难度：中
- 攻击路径：第三方软件漏洞 -> 使用该软件的云服务 -> 云服务系统/平台 -> 其他租户数据
- 利用方式：
  - ☑收集云服务利用的第三方软件列表与相应的版本信息，如MySQL，ElasticSearch，Docker，K8S等
  - ☑第三方软件0day研究和Nday的收集与利用
- 相关参考：
  - RDS (MySQL): https://paper.seebug.org/1112/

云自身为突破口

场景四：云服务私有或者公开API漏洞挖掘与利用

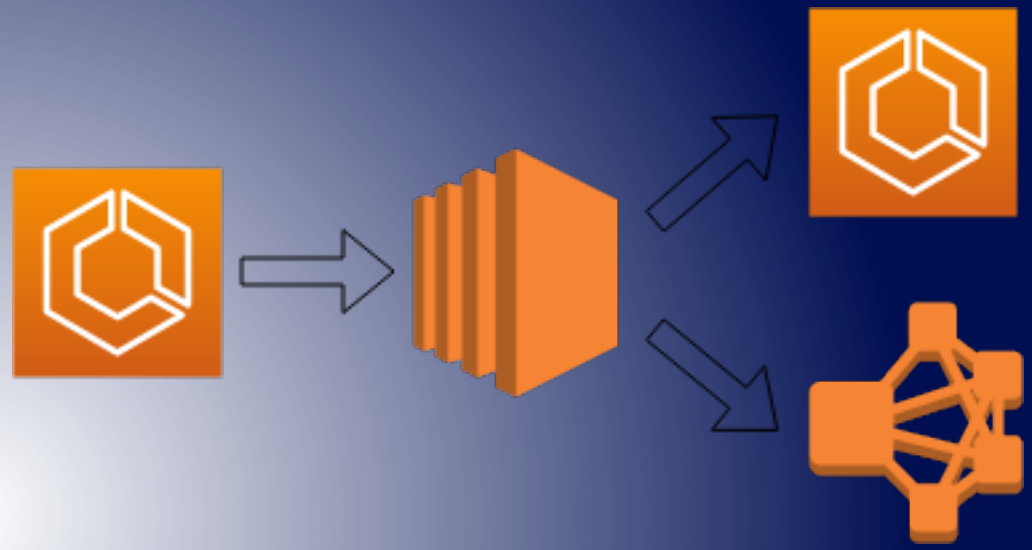
- 攻击难度：中-高
- 攻击路径：云主机中应用SSRF漏洞或者云服务账号AK/SK -> 云服务私有/公开API漏洞 -> RCE/信息泄露
- 利用方式：
  - ☑ 云服务私有API寻找与测试（云服务Web请求分析，云服务SDK或者离线工具分析等）
  - ☑ 云服务公开API漏洞研究（输入输出校验，认证与鉴权绕过等）
  - ☑ 云主机中的应用的SSRF漏洞
- 相关参考：
  - Azure:https://nosec.org/home/detail/4358.html
  - AWS:https://github.com/RhinoSecurityLabs/Cloud-Security-Research/tree/master/AWS/lambda_ssrf



云自身为突破口

场景五：容器逃逸

- 攻击难度：中-高
- 攻击路径：共享容器 -> 宿主机 -> 其他租户容器
- 利用方式：
  - ☑容器逃逸漏洞
  - ☑宿主机目录挂载
  - ☑特权容器
  - ☑Kubernetes安全
- 相关参考：
  - runC容器逃逸（CVE-2019-5736）: https://github.com/Frichetten/CVE-2019-5736-PoC, https://github.com/twistlock/RunC-CVE-2019-5736
  - Docker容器逃逸: https://www.exploit-db.com/exploits/47147
  - Docker容器逃逸之waitid()（CVE-2017-5123）:
  - https://github.com/nongiach/CVE/tree/master/CVE-2017-5123
  - GCP:https://github.com/RhinoSecurityLabs/Cloud-Security-Research/tree/master/GCP/cloud_shell_docker_escape
  - ATT&CK for Kubernetes: https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/



云自身为突破口

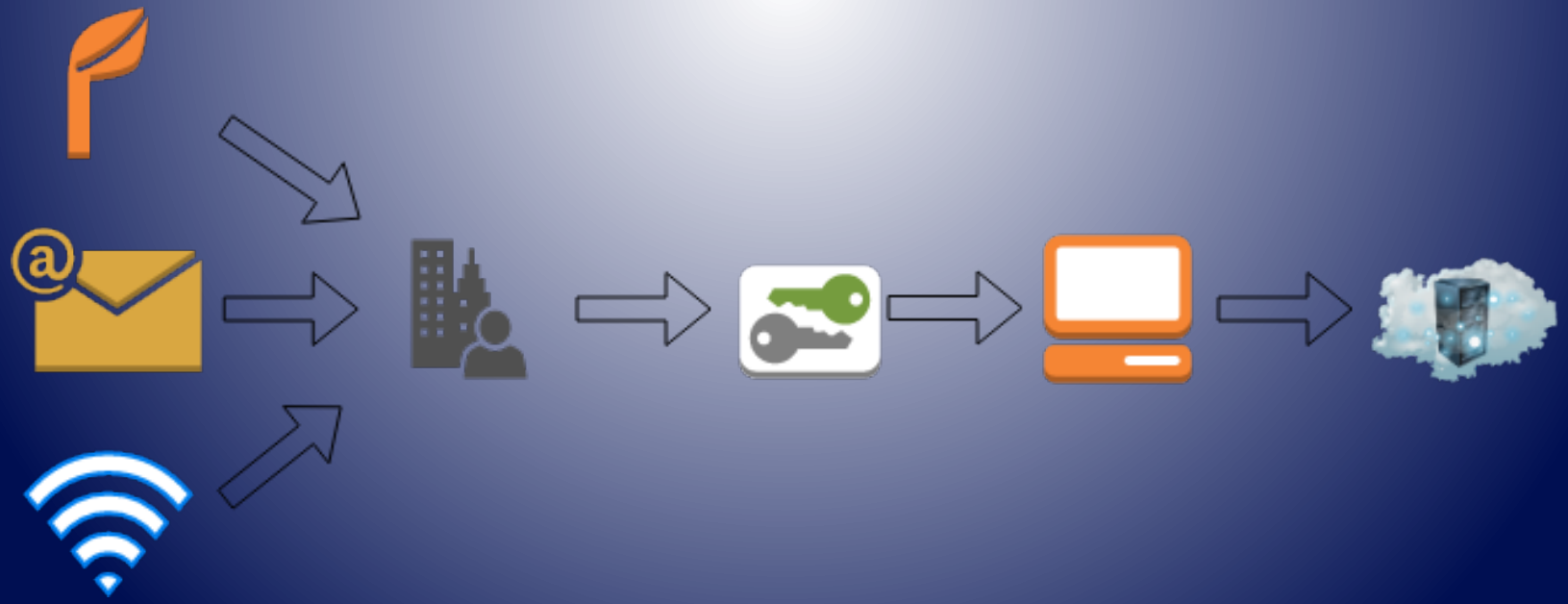
场景六：虚拟机逃逸

- 攻击难度：高
- 攻击路径：弹性云主机 -> 宿主机 -> 同一宿主机上其他弹性云主机
- 利用方式：虚拟机逃逸漏洞
- 相关参考：
  - QEMU逃逸漏洞: https://github.com/ray-cp/vm-escape/tree/master/qemu-escape
  - QEMU虚拟机逃逸漏洞分析与利用(CVE-2019-14378): https://www.anquanke.com/post/id/184949
  - QEMU虚拟机逃逸漏洞分析与利用(CVE-2019-6778): https://mp.weixin.qq.com/s/SgY1QsPmgU8iI4EUJfhznQ
  - QEMU虚拟机逃逸漏洞分析与利用(CVE-2015-5165, CVE-2015-7504, CVE-2015-7512): https://bbs.pediy.com/thread-217997.htm, https://bbs.pediy.com/thread-217999.htm, https://bbs.pediy.com/thread-218045.htm, https://www.freebuf.com/vuls/87673.html

云自身为突破口

场景七：云服务管理面网络入侵

- 攻击难度：高
- 攻击路径：公有云厂商办公网/DMZ区域 -> 公有云员工权限 -> 公有云管理面网络 -> 公有云生产网
- 利用方式：
  - ☑企业办公网/DMZ区域入口（钓鱼，OWA，VPN，WiFi，远程办公，物理入侵，DMZ区域对外应用漏洞等）
  - ☑传统的内网渗透入侵手法



安全+ 专注于安全行业，通过互联网平台、线下沙龙、培训、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站：

www.anquanjia.net.cn

微信公众号：anquanplus