CNIS
云网基础设施安全国家工程研究中心
National Engineering Research Center of Cloud and Network Infrastructure Security

2024 WEST LAKE DIGITAL SECURITY CONFERENCE
西湖论剑·数字安全大会 12th

靶场自动化安全评测能力解读

王帅

中国电信 CHINA TELECOM | 研究院 CTRI

网络靶场已成为主动化防御体系的关键组件

起源及发展

网络空间靶场最早于2008年出现在国家军事领域

随着国家网络战升级，网络靶场成为网络安全领域的重要装置

- 针对关键信息基础设施网络恶意攻击频发，攻击武器、攻击手法向高精尖演进，严重威胁国家安全
- 各国在网络空间对抗态势进一步加剧，相关国家网络空间政策的调整以及网络军事力量建设加速

业内靶场

各国加快建设网络安全靶场，促进网络安全人才队伍建设及攻防实战能力培养

- **美国：面向军民大力发展网络靶场，支撑网络安全的全生命周期服务**
- **欧安会：将靶场作为一种开发、交付和使用交互式仿真环境的平台**

国家靶场

- 2009年由DAPRA主导建设美国国家网络靶场（NCR）
- 于2010年10月发布的美国联邦网络空间靶场（FCR）
- 日本NICT的基平台（StarBED5）
- 北约网络空间靶场（NCR）

军事靶场

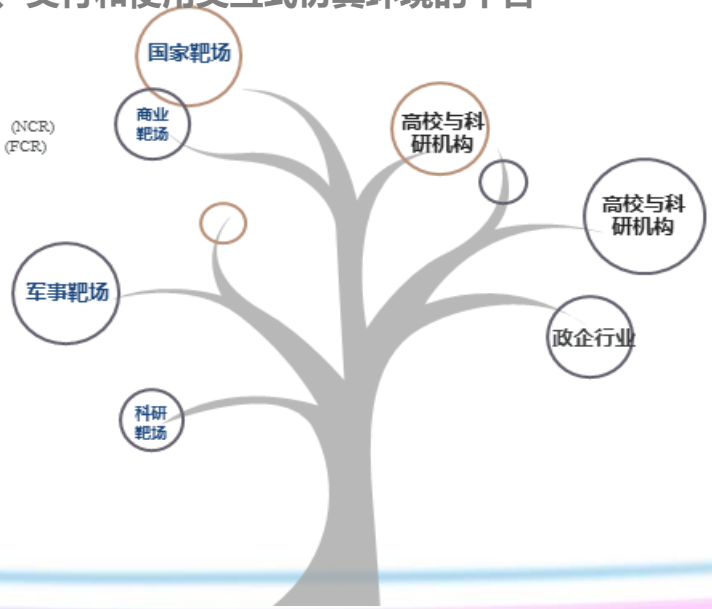
- 美军联合参谋部联合信息作战靶场（JIOR）
- 美军联合网络空间作战靶场（JCOR）
- 美国国防部靶场（CSR）

科研机构靶场

- 麻省理工大学Lincoln实验室
- 芝加哥大学Chameleon
- 美国自然科学基金CloudLab

商业公司靶场

- 英特尔公司Open Cirrus项目
- Cyberbit公司靶场
- 美国Circadence公司Project Ares®战神项目



靶场新方向

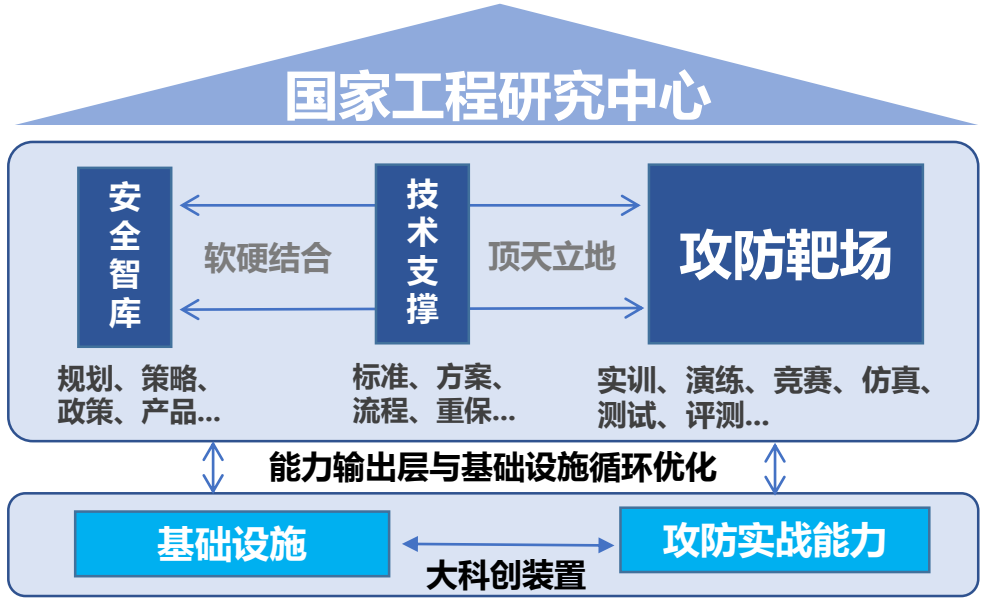
国内政策及靶场相关产业发展指导意见力度加大，对安全意识、技能、实训、演练、竞赛等要求进一步提升

涵盖安全测试、科学验证、安全评估等应用场景的**安全评测能力成为网络靶场新方向**

研究院已建成国内最大通信网络实体靶场

愿景

- ✓ 以网络靶场平台作为国家工程中心产业化的重要抓手，打造国家级云网基础设施安全评测基地
- ✓ 以“实战引领”为核心，研发综合性安全评测平台，构建全过程、全环节的安全评测体系，承接国家级安全评测任务，助力提升云网基础设施安全性



建设现状

一 个仿真基础设施

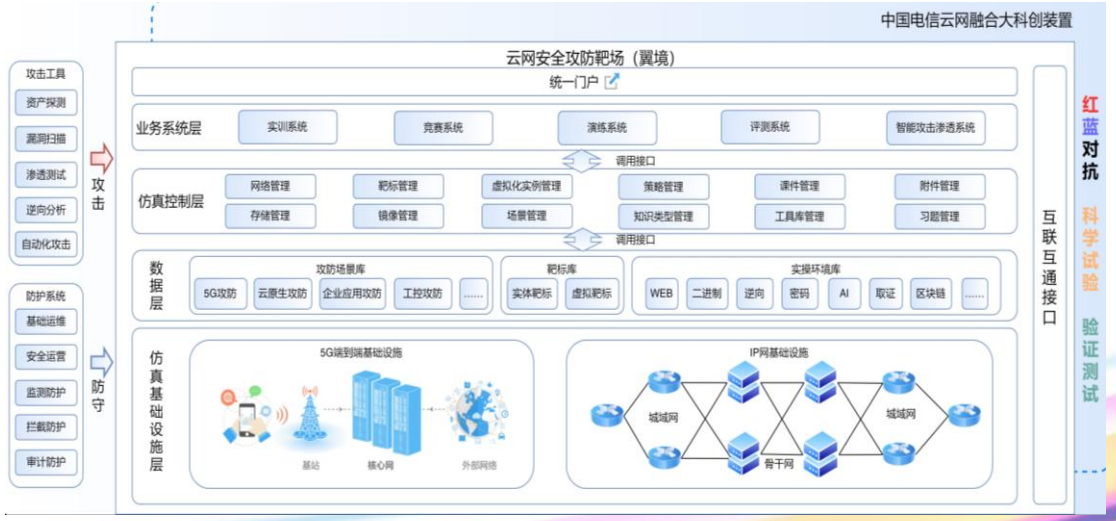
- ✓ 国内规模最大通信网络实体仿真基础设施，能力覆盖31省

四 大服务平台

- ✓ 安全试验平台
- ✓ 安全演练平台
- ✓ 安全实训平台
- ✓ **安全评测平台**

四 大服务能力

- 攻防演练：贴近现网的红蓝对抗、关基攻防、极限场景等实战演练
- 科学试验：基于大规模仿真环境的安全新技术新架构、网络武器等试验验证
- 攻防实训：基于云网攻防实战的人才培养与选拔
- **安全评测：面向仿真、现网环境的全面、深度、高效自动化安全评测**



以智能攻击渗透打造自动化靶场安全评测能力

智能高效、覆盖全面、攻防对抗的自动化安全评测能力

- 中国电信研究院自主研发，基于ATT&CK攻防技战法，覆盖信息收集、扫描探测、漏洞验证与利用、横向移动、内网渗透全生命周期安全测试，能够自动进行漏洞扫描、漏洞利用、横向渗透等一站式安全评测，并可结合靶场仿真环境与业务平台开展自动化攻击模拟测试，可有效对特定业务系统的安全防护体系进行评测

Assets
资产探测引擎、
攻击面风险监测引擎

Detect
无感漏洞检测引擎、
数据安全检测引擎...

Attack
自动攻击模拟引擎、
横向渗透引擎...

Plugins
自适应加载插件

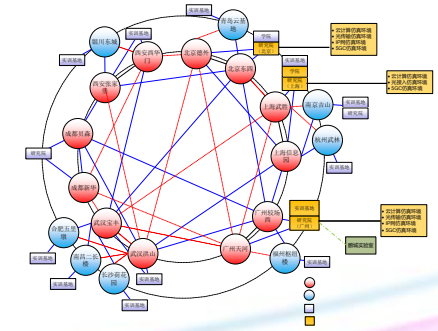
Evaluate
综合评测

能力引擎

基于ATT&CK攻防技战法

一站式

仿真基础设施环境



现网实体设施环境

功能框架

自动化安全评测功能框架主要包括数据存储层、核心能力层和系统接入层，集成安全扫描、漏洞检测、漏洞利用、横向渗透、攻击面风险监测、数据安全检测等核心安全能力，可针对企业各类资产和产品提供全面、动态、持续性的安全评测

六大核心能力模块

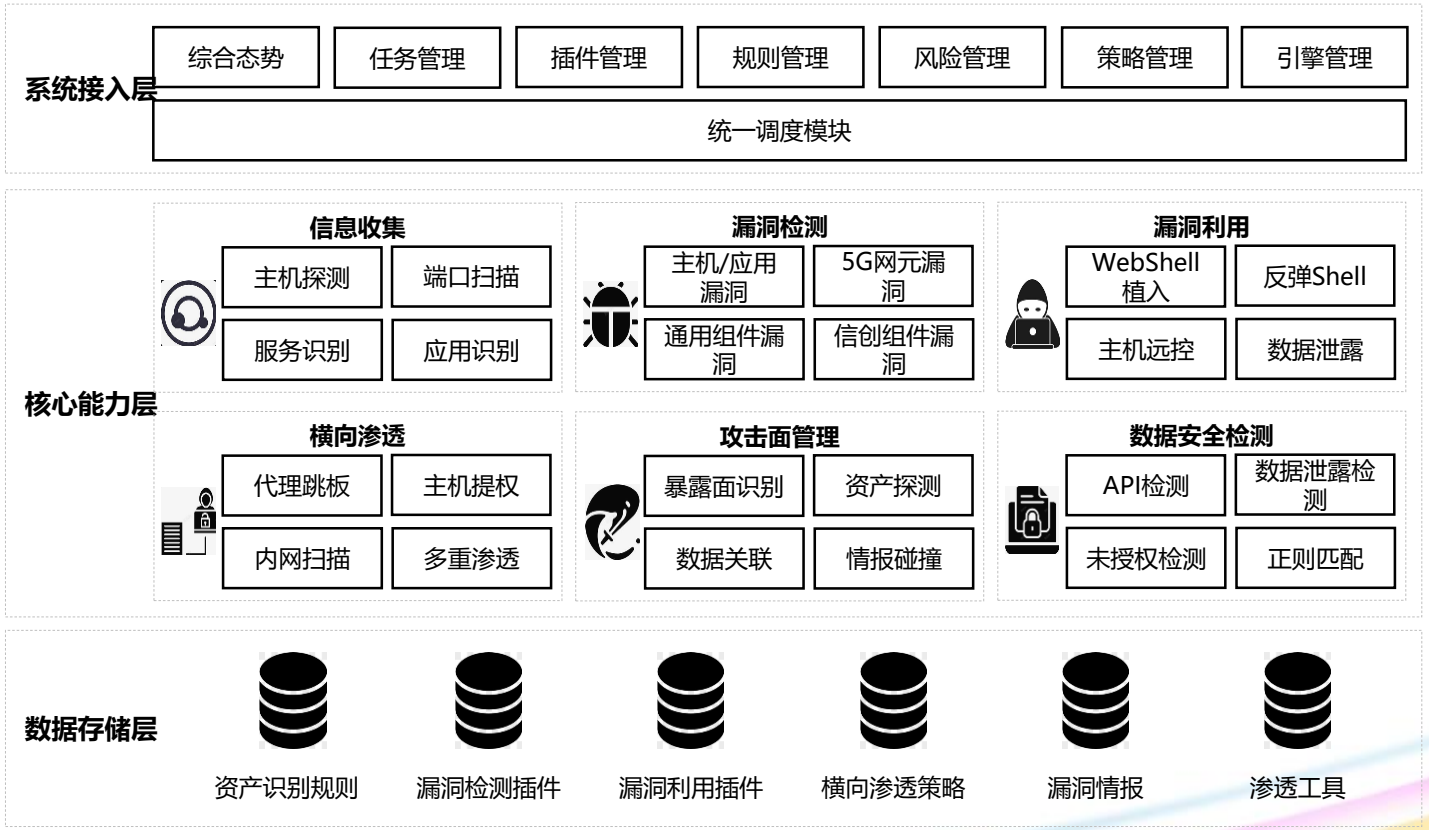
- 能力层包含信息收集、漏洞检测、漏洞利用、横向渗透、攻击面管理、数据安全探测六大模块，涵盖渗透测试全流程，模拟黑客攻击手法，实现主动风险探测，全面深入发现和评估网络和系统安全风险

六大核心数据库

- 数据存储层包含能力引擎依赖的资产识别规则、漏洞检测插件、漏洞利用插件、渗透策略、漏洞情报和渗透工具等数据库，为实现资产探测、漏洞发现、漏洞利用、攻击全景可视化等安全评测能力提供支撑

七大业务管理功能

- 接入层涵盖综合态势、任务管理等七大业务功能，并提供可视化风险评测过程和结果，通过统一调度模块与后端核心能力引擎交互

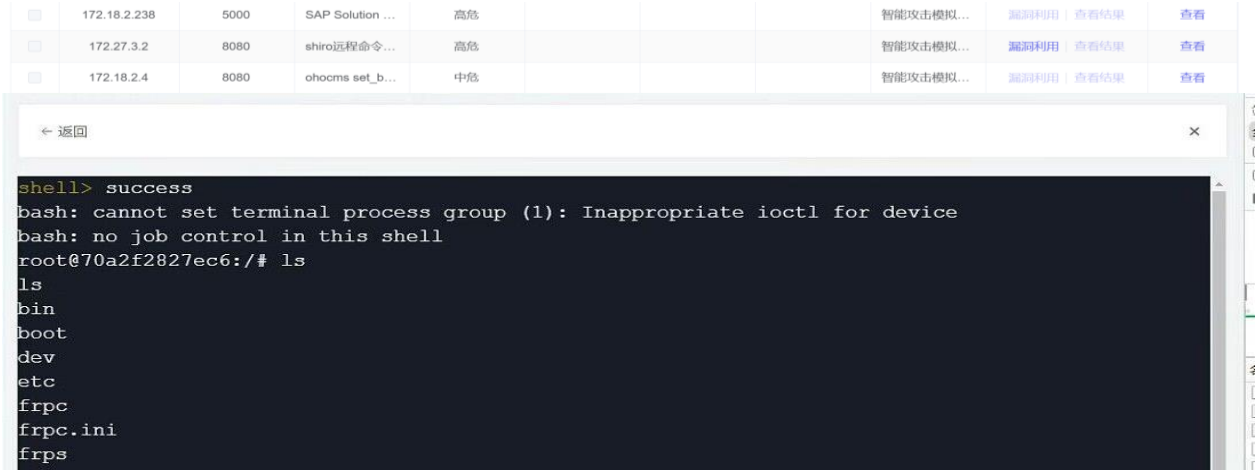


关键技术及创新（1/2）

在传统的漏洞风险扫描检测能力的基础上，采用**高危漏洞深度利用**与**基于ATT&CK攻击技术的智能渗透策略**来实现**安全扫描、漏洞检测、漏洞利用、横向渗透、攻击面检测、数据安全检测**等多阶段、全流程、自动化的攻击模拟能力

□ 多方式深层次的自动化漏洞利用

- 在传统的漏洞检测能力基础上，针对远程代码执行、文件上传、任意文件读取、未授权访问等高危漏洞**执行主机控制、代理植入、获取数据等深度利用**，全面模拟攻击者对系统的控制权获取与持久化等攻击行为，**为进一步开展横向移动、纵深提权提供跳板环境**



□ 基于ATT&CK的攻击技战术模拟

- 基于ATT&CK攻击技术框架来模拟攻击者行为，系统内置**涵盖边界突破、权限提升、权限维持、横向移动、数据窃取等关键技战术的攻击模拟策略**，覆盖5G、云、信创、开源组件等新技术新应用场景，真实模拟攻击者面对业务整体安全体系的攻击手段和路径，**全方位发现业务潜在的攻击面和安全能力短板**

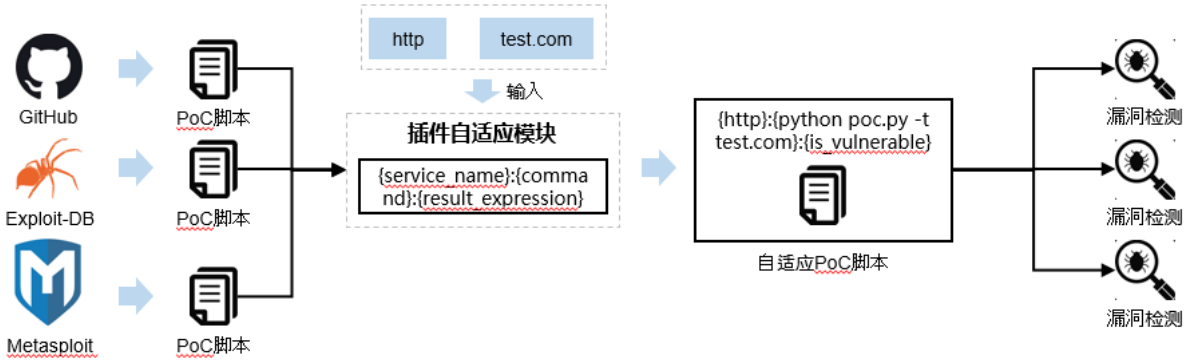
14个战术、196个技术、411个子技术

关键技术及创新（2/2）

针对当前业界主流漏洞扫描与自动化攻击模拟系统存在**漏洞检测能力集成效率低、漏洞扫描检测能力单一**等问题，导致对业务安全体系的**评测工作存在效率不高、深度不足的现象**，因此创新提出**漏洞插件快速集成与漏洞智能利用**等技术来提升安全评测效能。

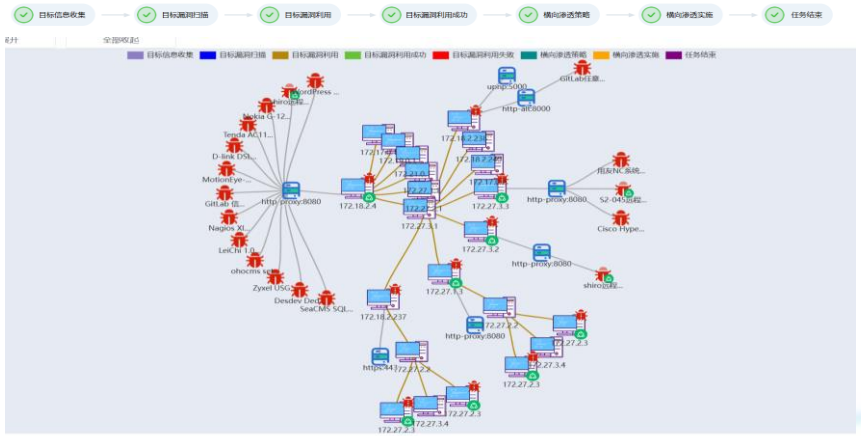
□ 快速自适应漏洞插件驱动技术

创新研发基于多语言环境的漏洞插件自适应引擎，通过自适应生成漏洞插件的运行指令，安全运营人员可以**不受检测系统的插件开发规范的限制，快速集成自研或外部引用的漏洞检测和利用插件**，实现新发漏洞检测能力快速集成能力由**小时/天提升至分钟级，**大幅提升对新发漏洞的攻击面筛查效率



□ 多重网络自动化横向渗透技术

创新提出基于多层代理与流量转发的多重网络自动化横向渗透技术，通过对边界失陷主机利用多层代理与流量转发技术**打通多重内网隧道，自动对内网进行侦察扫描、漏洞检测、权限提升、命令执行与控制等，**实现对内网进行迭代横向渗透，扩大攻击战果，提升影响范围



应用场景及案例（1/2）

能力服务简介

- **基础安全评测**

基于丰富的攻防知识库、工具库等资源，可提供针对业务系统与信创产品开展**漏洞众测、风险评估、安全功能/性能测试**等基础评测内容

- **业务安全能力评测**

通过实时控制交互、多重网络自动化渗透等能力，可以面向关基设施网络及业务系统的**涵盖网络、系统、应用层面提供整体安全能力评测**

典型应用场景

安全能力评测

5G网络安全能力评测

云原生安全能力评测

IP网业务安全能力评测

工控应用安全能力评测

安全漏洞众测

对外服务系统安全众测

信创产品组件漏洞挖掘

信创安全评测

信创产品安全风险评估

信创安全产品能力评估

应用场景及案例（2/2）

□ 典型应用案例

- **面向中国电信互联网暴露面资产开展主动安全评测**

  通过云化部署方式面向中国电信全网互联网暴露面资产开展主动风险检测，帮助中国电信全网发现有效中高危漏洞

- **面向中国电信省级公司开展重要业务系统安全评测**

  在湖南、广东、浙江、辽宁、山东、福建、海南等多家电信省公司开展试点应用，对重要业务系统进行安全能力评估，帮助各省提升安全能力建设和运营工作效率

- **中国电信自研与集采产品安全评测**

  对中国电信研发云、翼枢SASE、态势感知、重保系统、云WAF，以及微隔离、信创操作系统等产品开展安全评测，促进中国电信自研及采购产品安全水平提升

成果特色总结

智能高效、覆盖全面、攻防对抗

业界首次实现黑客视角下自动化完整攻击链渗透，大幅节约人力成本

创新一键探测、一插即用、横向渗透技术，大幅提升安全评测效率

5G、云、信创、开源组件等新技术新应用场景全覆盖，应用前景广泛

CNIS
云网基础设施安全国家工程研究中心
National Engineering Research Center of Cloud and Network Infrastructure Security

2024 WEST LAKE DIGITAL SECURITY CONFERENCE
西湖论剑·数字安全大会 12th

征程万里风正劲
重任千钧再奋蹄