新一代自动化渗透平台的设计与实现

cnrstar@四维创智

www.4dogs.cn

自我介绍

- 8年渗透测试实战经验
- 常年奋斗在渗透测试前线
- 带领公司致力于自动化渗透测试研究
- 任职于四维创智(国家信息安全技术研究中心战略合作伙伴)，完成多个国家级项目

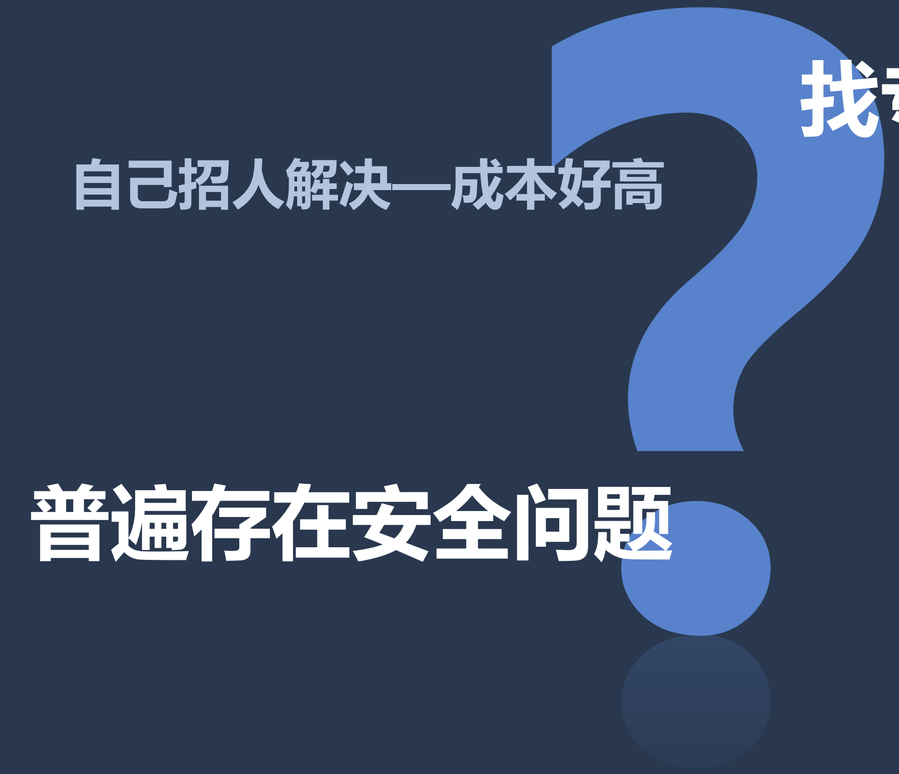
为什么要做自动化渗透

渗透测试人员面临的问题

防火墙　　IDS　　W　　威胁感知与流量监控

渗透越来越难　　成本越来越高

企业面临的问题



找专业公司解决—好贵

自己招人解决—成本好高

如何破？

普遍存在安全问题

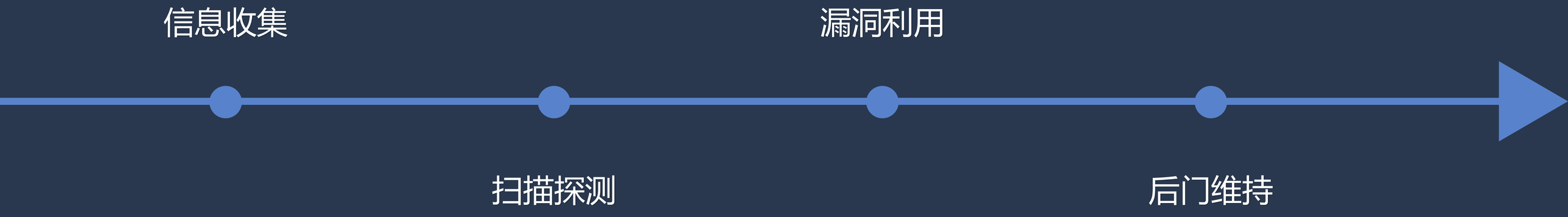
新一代自动化渗透测试平台

渗透测试三字经

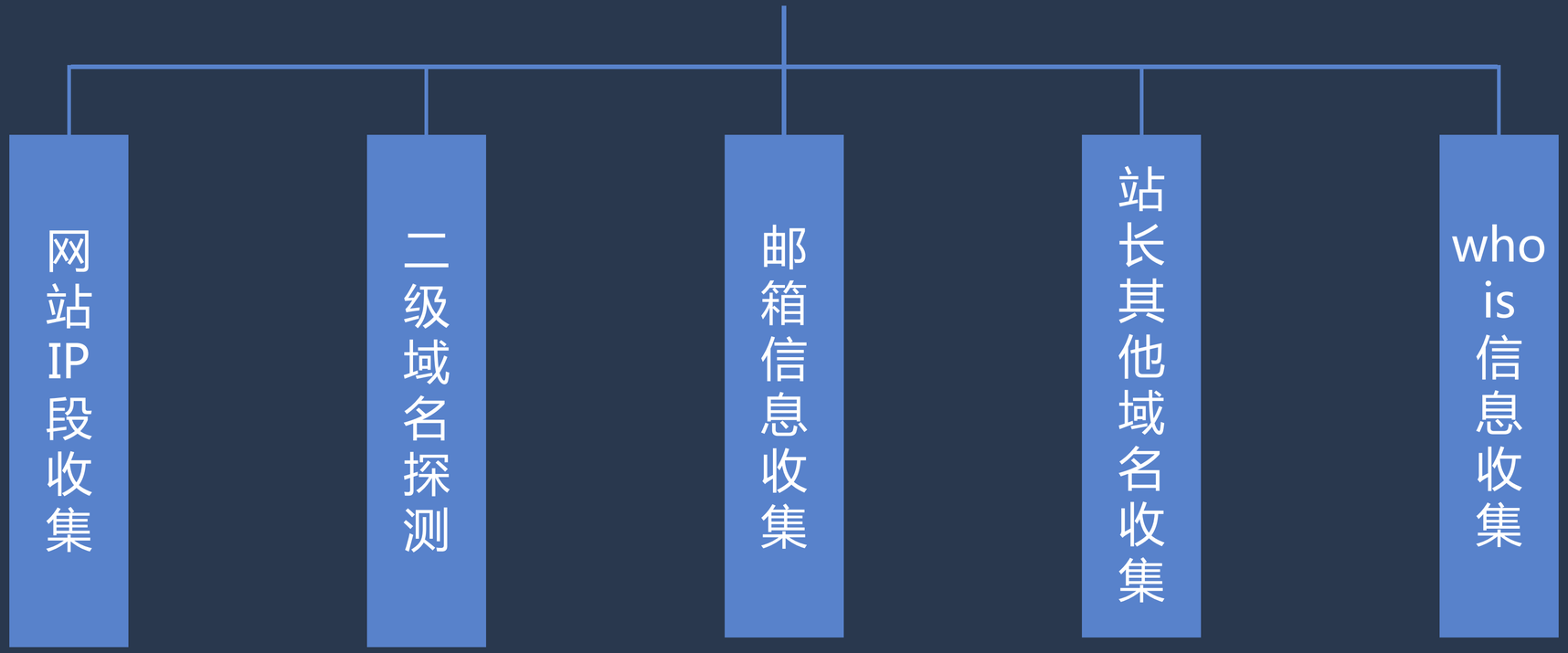
进谷歌 找注入　　没注入 就旁注　　没旁注 用Oday　　没Oday 猜目录　　没目录 就嗅探

拿不下 去自杀　　爆账户 找后台　　传小马 放大马　　拿权限 挂页面　　放暗链 清数据

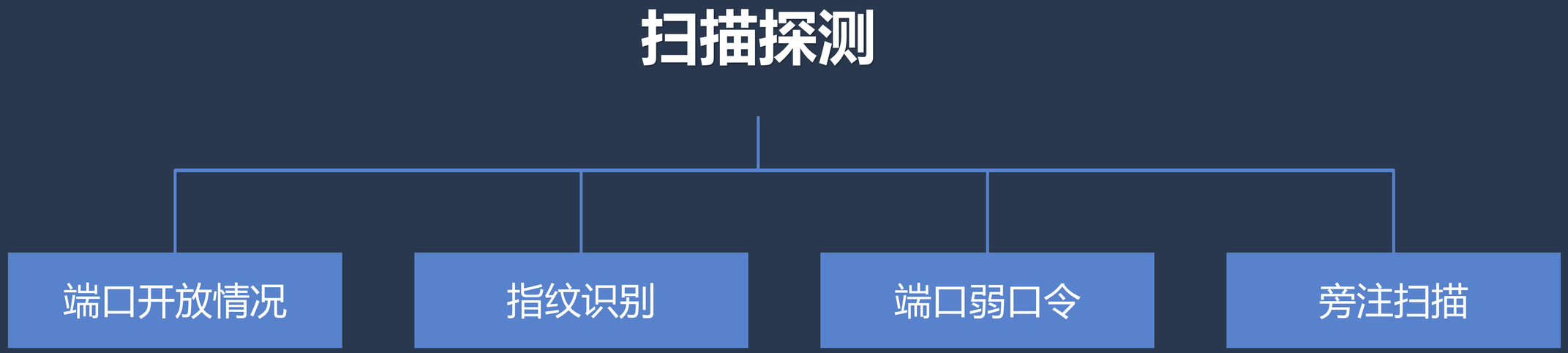
渗透测试流程-大套路



信息收集套路



扫描探测套路



漏洞利用套路

自动化渗透来了

要达到的效果

- 给定一个目标—获取到所有可能获取的菜刀shell Or 种植远控
- 搞不定的，输出可能利用的点

我们的资源

nmap扫端口、hydra破密码、whatweb识别指纹、Burp抓包、msf利用漏洞、御剑扫描目录、set搞社工、awvs扫漏洞、sqlmap穿山甲搞注入、K8搞Struts2、菜刀控shell...

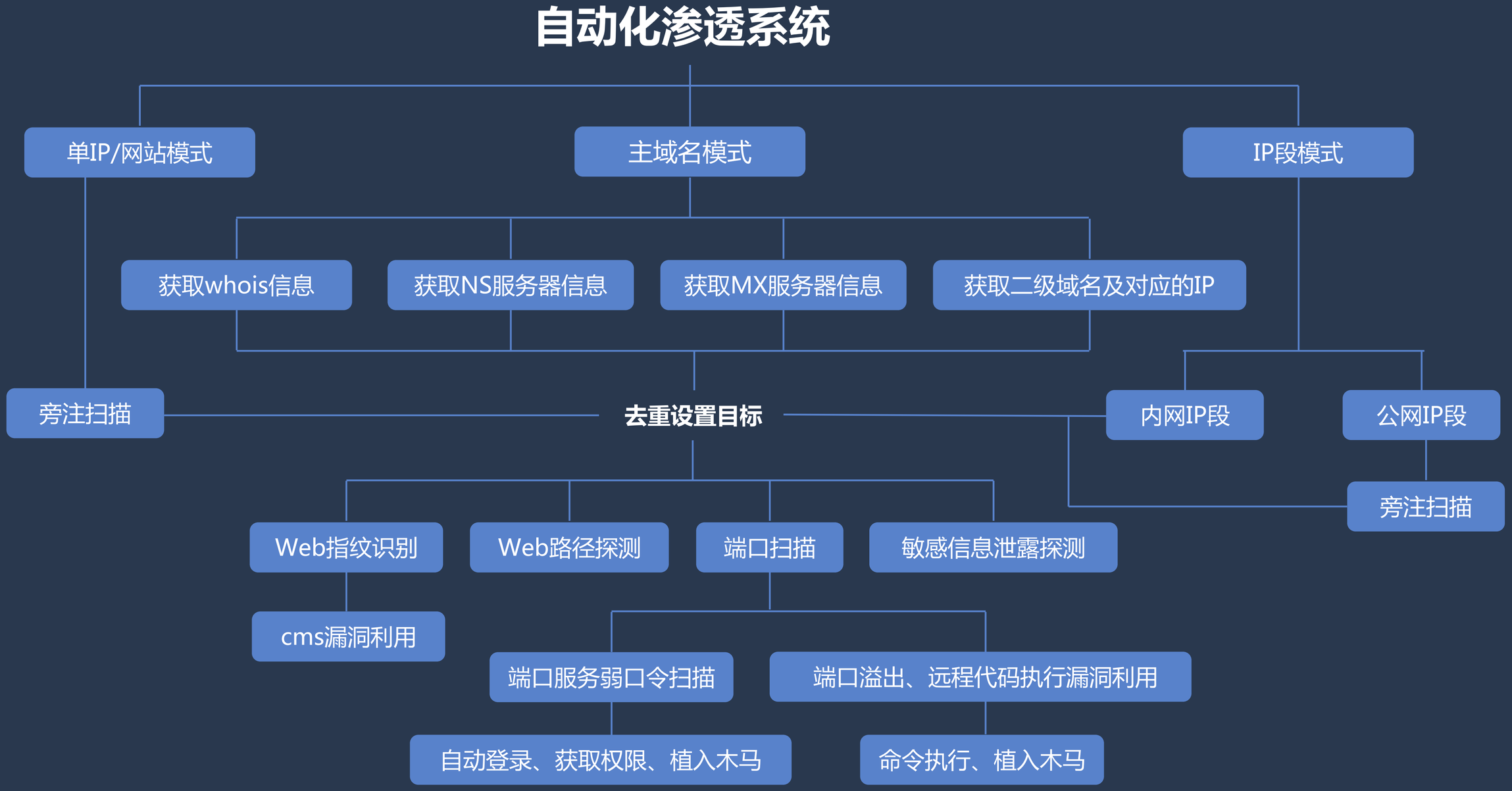
各类独立工具

功能有、可独立利用

面临的问题

- 无独立调用接口
  - 工具由各种语言编写(java、C、C++、C#、php、Python...)
  - 如何联动？
- 面对WAF如何破？

基本思路架构


自动化渗透系统
单IP/网站模式
主域名模式
IP段模式
获取whois信息
获取NS服务器信息
获取MX服务器信息
获取二级域名及对应的IP
旁注扫描
去重设置目标
内网IP段
公网IP段
旁注扫描
Web指纹识别
Web路径探测
端口扫描
敏感信息泄露探测
cms漏洞利用
端口服务弱口令扫描
端口溢出、远程代码执行漏洞利用
自动登录、获取权限、植入木马
命令执行、植入木马

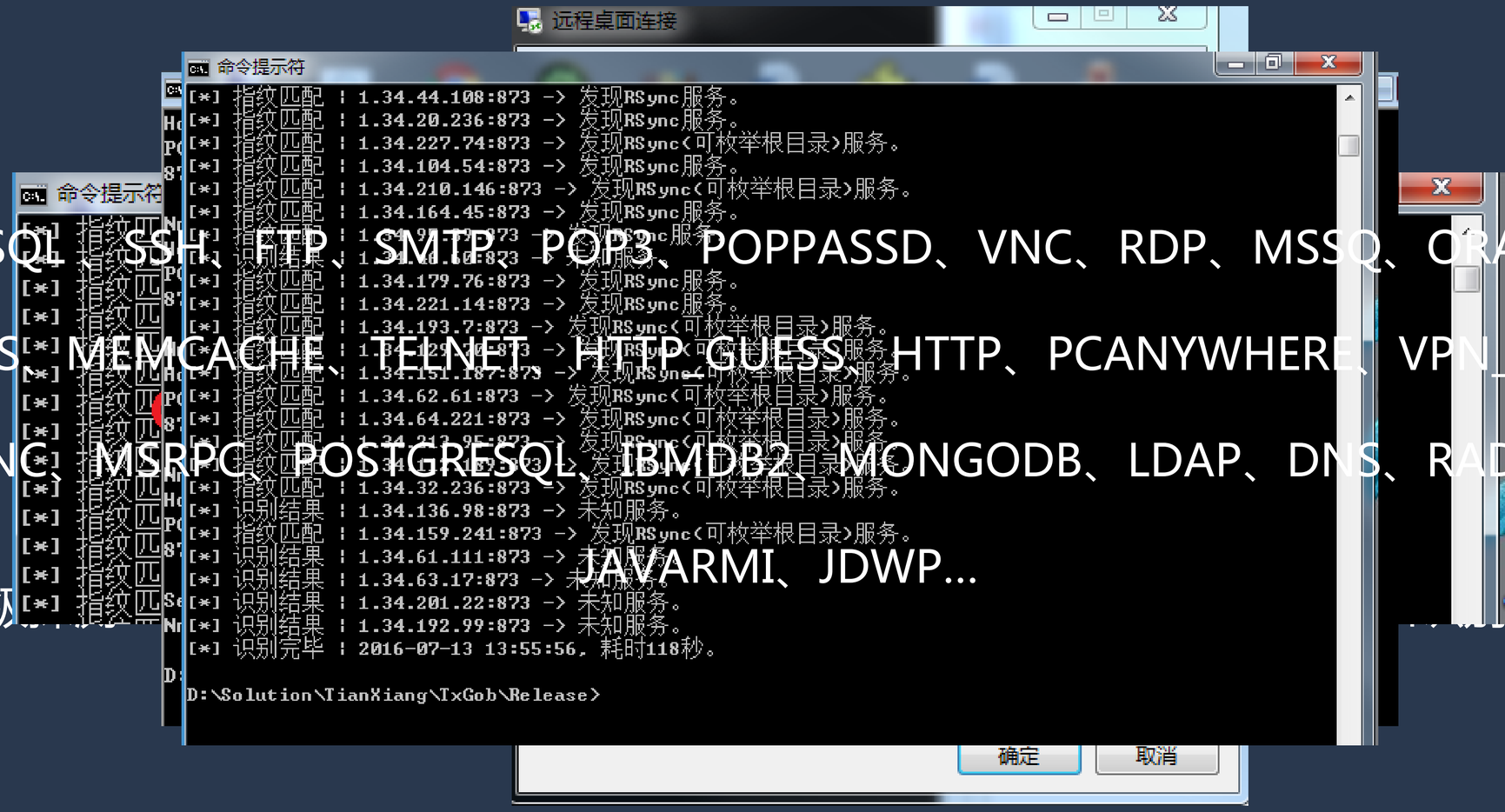
联动后的优势

- 收集到二级域名、相关域名-自动生成目标IP段
- 识别到端口开放—自动调用爆破工具、利用工具进行探测
- 收集到邮箱-自动关联社工库历史数据探测
- 识别到jboss-自动getshell
- 识别到CMS-自动尝试漏洞库已有exploit，输出利用结果

那些坑

- 菜刀遇到WAF-无法连接
- 端口扫描碰到防火墙-所有端口似乎都开着
- 路径扫描碰到WAF-所有路径似乎都存在

防火墙处理



MySQL、SSH、FTP、SMTP、POP3、POPPASSD、VNC、RDP、MSSQ、ORACLE、REDIS、MEMCACHE、TELNET、HTTP GUESS、HTTP、PCANYWHERE、VPN_PPTP、RSYNC、MSRPC、POSTGRESQL、IBMDB2、MONGODB、LDAP、DNS、RADMIN、JAVARMI、JDWP...

- 轻量级 率提高40%

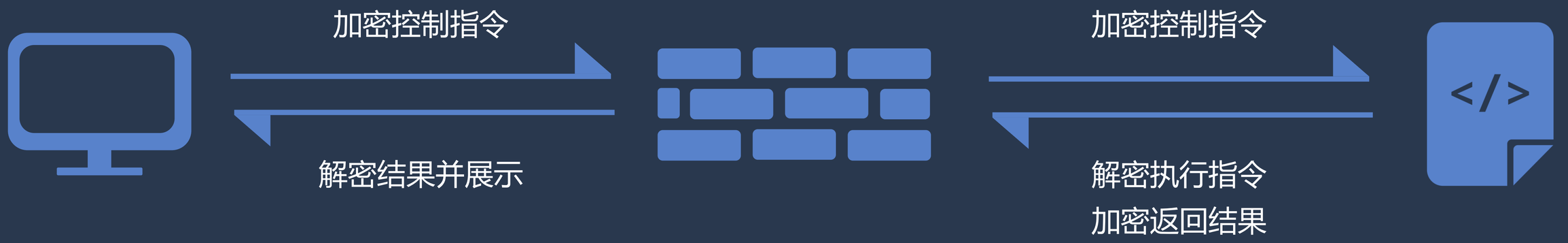
WAF处理

智能自动化识别WAF

自动放弃功能

Webshell处理

双向加密绕过WAF过滤



Thanks

cnrstar@四维创智