网络安全 FCIS 2023 创新大会

红队反溯源与安全线路建设

自由安全研究员

伍智波（SkyMine）

FREEBUF

- 伍智波（SkyMine）
- 自由安全研究员，“全栈红队”公众号主理人，某公益计划资助人
- KCon/HITB/FIT/CIS 演讲者，GeekPwn 获奖者，Security+/CISP-PTS/CISP/CISAW/CIIT/CDPSE 证书持有者
- 6年安全实验室管理和红蓝对抗实战经验，连续3年国护攻击队队长，数十场高级别攻防演练攻击队队长
- 擅长内外网渗透、钓鱼、安全开发、取证、实验室/红队/蓝军建设管理
- PADI名仕潜水员（全球TOP 2%）

01 红队被溯源案例

02 红队常见的反溯源策略

03 IP反溯源及安全通讯线路建设

【案例1】红队被JSONP蜜罐反制

浏览器已登陆X度网盘
缓存了X度账号cookie

误点JSONP蜜罐，蜜罐盗用
X度cookie获取X度账号ID

用X度账号ID在社工库
匹配真实身份信息

【案例2】红队钓鱼邮服被反制

红队使用Ewomail软件
部署了一个自建邮服
用于发送钓鱼邮件

蓝队捕获钓鱼邮件
查看邮件头X-Originating-IP字段
找到红队自建邮服IP地址

Ewomail软件存在默认口令
红队邮服被蓝队反控

【案例3】红队被定位公司身份

红队在公司进行远程攻击
使用公司宽带网络出口

蓝队在安全设备抓到IP
通过IP数据查到公司位置
在这个位置只有1家安全公司

蓝队让甲方联系该公司销售
谎称了解技术能力
套出正在进行某演练的红队

【案例4】红队使用CS4.7攻击机被蓝队反制

红队在VPS上部署CS 4.7
生成木马投放钓鱼

蓝队抓到木马样本
利用CVE-2022-39197
构造上线

红队CS4.7收到上线会话
使用task list功能时触发EXP
蓝队RCE反控红队攻击机

【案例5】红队使用代理隐藏身份后仍被溯源

网络代理商配合防守方
提供IP实名信息和路由日志

- 中国：《网络安全法》第三章第一节第二十一条、第二十八条
- 美国：《美国爱国者法案》206、207、215、702条
- 英国：《刑事调查和监测法》53-54、56-57、58-59条
- 俄罗斯：《俄罗斯联邦刑法典》第138.1条
- 法国：《信息与自由法》第L851-1条、第L852-1条、第L854-1条

01 红队被溯源案例

02 红队常见的反溯源策略

03 IP反溯源及安全通讯线路建设

浏览器反溯源：对抗JSONP蜜罐

浏览器隐私模式不会使用已保存的cookie

Jsonp没有cookie不能正常利用

使用独立的浏览器进行攻击操作，如日常上网用Firefox，攻击用Chrome

*反蜜罐浏览器插件兼顾了便利性，但由于覆盖面有限，安全性不如上述措施

浏览器反溯源：对抗BurpSuite反制

低版本BurpSuite内置低版本的Chromium

Repeater-Render位置 1Click 触发RCE

JavaScript analysis功能 0Click 触发RCE

积极将BurpSuite随时更新至最新版本

新版本BurpSuite会更新Chromium版本

浏览器反溯源：浏览器数据转储

红队人员电脑意外被控

浏览器历史数据被转储

严格遵守红队工作纪律红线

使用独立虚拟机进行攻击

社交媒体反溯源：MySQL蜜罐读取红队微信号

红队找到一个外网/内网数据库

果断Navicat连上准备拿数据分

MySQL蜜罐读取C:\Windows\PFRO.log寻获用户名，

读取C:\Users\username\Documents\WeChat Files\

All Users\config\config.data寻获微信号

*应当严格遵守红队工作纪律红线，使用独立虚拟机进行攻击

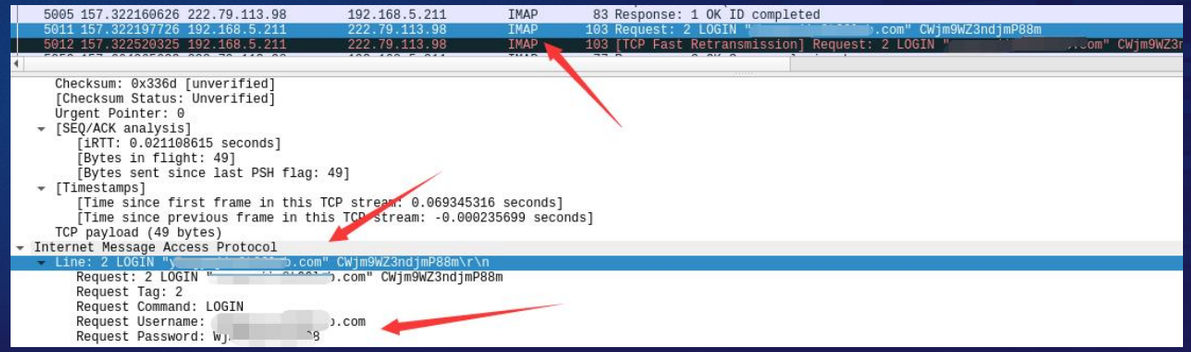
社交媒体反溯源：内网渗透泄露攻击机邮箱信息

红队撕开口子代理进内网

但误用全局代理

攻击机全局流量进入目标内网

流量中的IMAP/POP3报文泄露邮箱



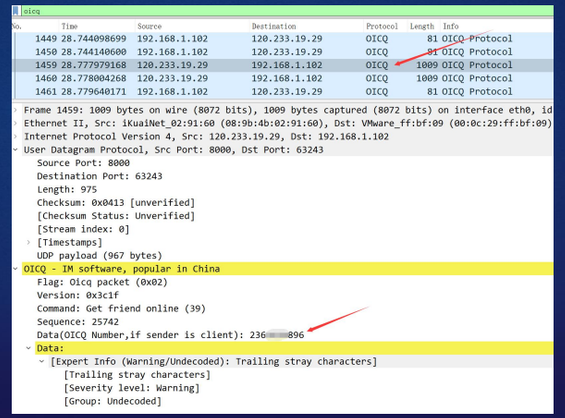
社交媒体反溯源：内网渗透泄露攻击机QQ号

红队撕开口子代理进内网

但误用全局代理

攻击机全局流量进入目标内网

流量中的OICQ报文泄露QQ号



使用局部代理

使用独立虚拟机攻击

社交媒体反溯源：微信聊天记录被导出

红队人员电脑意外被控

微信聊天记录被导出

严格遵守红队工作纪律红线

使用独立虚拟机进行攻击

基础设施反溯源：防止远控服务器被反制

使用域前置、云函数

隐藏C2真实IP

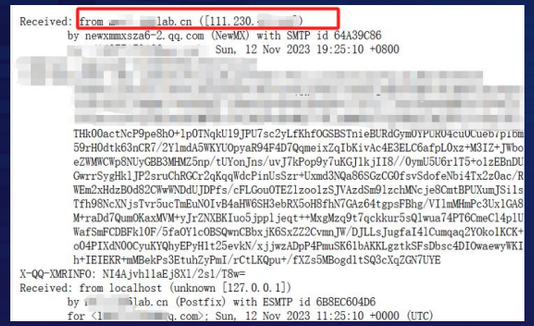
teamserver杜绝弱口令

使用自定义端口

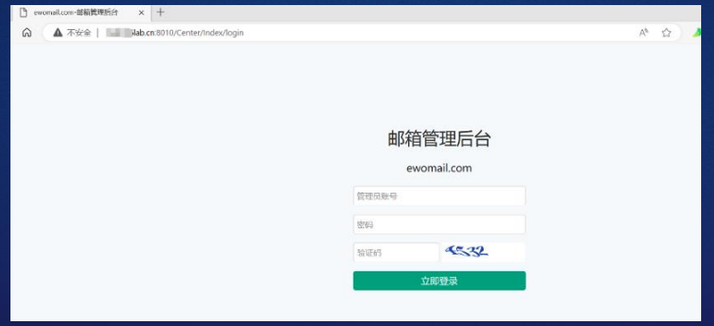
专机专用

不与其他基础设施混用

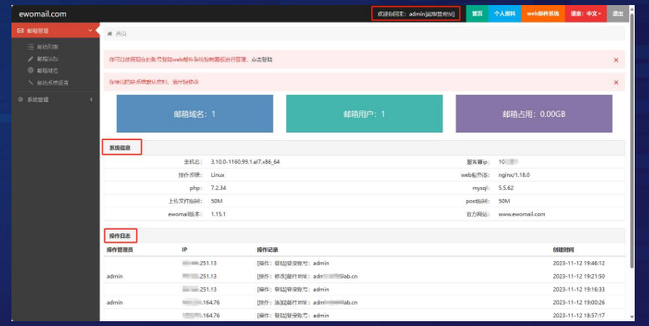
基础设施反溯源：钓鱼邮服被反制



钓鱼邮件原文泄露邮服IP



访问钓鱼邮服IP发现ewomail软件



Ewomail存在默认密码，反制红队邮服

基础设施反溯源：防止钓鱼邮服被反制

使用可靠的邮服软件

163

使用第三方托管邮服

专机专用

不与其他基础设施混用

01 红队被溯源案例

02 红队常见的反溯源策略

03 IP反溯源及安全通讯线路建设

IP地址溯源风险

IP关联地理定位

电信商配合防守方
提供IP实名信息

软件配合防守方
提供IP关联信息

网络代理商配合防守方
提供IP实名信息

国内攻防演练场景下的安全线路建设

*使用多个云服务商作为节点来搭建线路

跨国犯罪侦查场景下的安全线路建设

*使用多个国家、多个云服务商作为节点来搭建线路

传统多跳代理网络方案——多层VPN 3跳

SecNet

多跳点反追踪安全线路搭建工具

[免费、一键、简单、红队专用的]

SecNet —— 多跳点反追踪安全线路搭建工具

11.11.11.11

22.22.22.22

33.33.33.33

自备若干台干净的VPS，有多少台就是多少跳，示例演示3跳

操作系统要求：CentOS 7+ / Ubuntu 18+

*基于相关法律法规，本程序不能在中国大陆以外的VPS上运行

SecNet —— 多跳点反追踪安全线路搭建工具

11.11.11.11
第一跳
（入口点）

22.22.22.22
第二跳
（中间节点）

33.33.33.33
第三跳
（出口点）

首先在作为入口点的VPS上执行一键安装命令（见最后一页）

按照提示，输入第二跳IP地址22.22.22.22

SecNet —— 多跳点反追踪安全线路搭建工具

11.11.11.11
第一跳
（入口点）

22.22.22.22
第二跳
（中间节点）

33.33.33.33
第三跳
（出口点）

然后在作为中间节点的VPS上执行一键安装命令（见最后一页）

按照提示，输入第三跳IP地址33.33.33.33

SecNet —— 多跳点反追踪安全线路搭建工具

11.11.11.11
第一跳
（入口点）

22.22.22.22
第二跳
（中间节点）

33.33.33.33
第三跳
（出口点）

最后在作为出口点的VPS上执行一键安装命令（见最后一页）

安装完成，获得一个openVPN账号密码

SecNet —— 多跳点反追踪安全线路搭建工具

此时3个节点（3跳）已经被串起来了

使用openVPN账号密码连接入口点IP 11.11.11.11即可接入安全线路

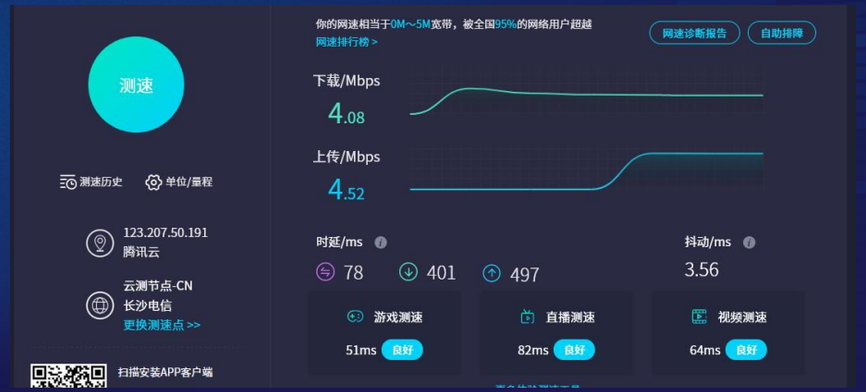
此时用ip138查IP显示的是出口点IP 33.33.33.33

SecNet —— 多跳点反追踪安全线路搭建工具 3跳

11.11.11.11
第一跳
（入口点）

22.22.22.22
第二跳
（中间节点）

33.33.33.33
第三跳
（出口点）

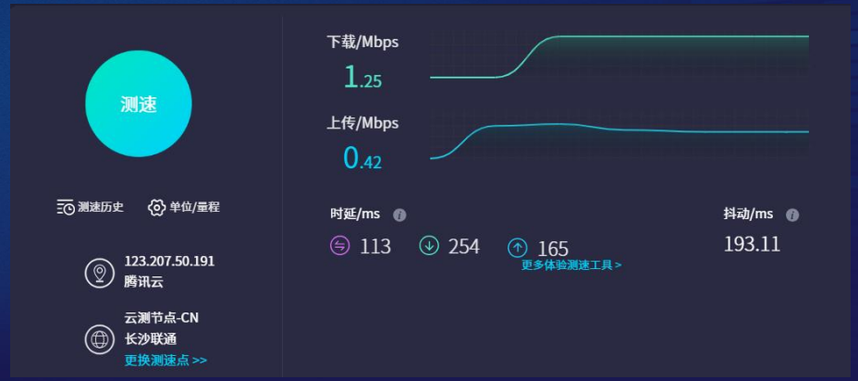


SecNet —— 多跳点反追踪安全线路搭建工具 6跳

11.11.11.11
第一跳
（入口点）

第2、3、4、5跳
（中间节点）

66.66.66.66
第六跳
（出口点）



自搭建安全线路的局限

支付身份风险

中间通信安全性

中间节点隐蔽性

线路通讯体验

深度优化安全线路

使用AES256全链路加密

中间节点部署仿真业务

自研私有通讯协议
解决TCP固有缺陷

多链路负载均衡
节点优选

深度优化安全线路 3跳

11.11.11.11
第一跳
（入口点）

22.22.22.22
第二跳
（中间节点）

33.33.33.33
第三跳
（出口点）

深度优化安全线路 6跳

11.11.11.11
第一跳
（入口点）

第2、3、4、5跳
（中间节点）

66.66.66.66
第六跳
（出口点）

国内场景——优化效果对比（4M带宽接入）

	传统方案 3跳	传统方案 6跳	SecNet 3跳	SecNet 6跳
下行速率均值（MB/s）	0.17	0.03	0.82	0.16
下行速率峰值（MB/s）	0.22	0.05	1.21	0.20
折合带宽均值（Mbps）	1.33	0.31	4.08	1.25
Ping时延均值（ms）	291	751	78	113

跨国场景——优化效果对比（100M带宽接入）

	传统方案 3跳	传统方案 6跳	SecNet 3跳	SecNet 6跳	深度优化方案 3跳	深度优化方案 6跳
下行速率均值（MB/s）	0.15	0.06	0.82	0.20	12.37	12.19
下行速率峰值（MB/s）	0.20	0.11	1.21	0.29	12.61	12.70
折合带宽均值（Mbps）	1.22	0.50	6.57	1.59	98.96	97.59
Ping时延均值（ms）	615	920	399	510	29	68

议题总结

- 浏览器反溯源：
  - 开启浏览器的隐私模式
  - 使用独立浏览器进行攻击
- 社交媒体反溯源：
  - 打内网时禁止全局代理
  - 使用专用虚拟机进行攻击
- 基础设施反溯源：
  - 使用域前置、云函数隐藏C2 IP
  - 专机专用，~~申请充足的项目预算~~
- IP反溯源：
  - 不使用单位网络出口进行攻击
  - 使用SecNet多跳安全线路进行攻击

关注“全栈红队”公众号
回复**231123**
获取**SecNet安装教程**、**PPT**及**议题文章**

网络安全 FCIS 2023创新大会

THANKS

关注“全栈红队”公众号

回复**231123**

获取**SecNet安装教程**、**PPT**及**议题文章**

FREEBUF