# Red Team Infrastructure Tips

红队基础设施的一些探讨

Date: 2020/11/14
Address: Shenzhen

# 自我介绍

## 李木

黑白天实验室安全研究员
Freebuf专栏作者
在读大学生
一个菜弟弟

# 什么是红队？

红队的概念最早来源于20世纪60年代的美国军方，原文定义如下：

An independent group that challenges an organization to improve its effectiveness by assuming an adversarial role.

翻译过来的大致意思是：
一个通过承担对抗性角色来挑战组织以提高其有效性的独立的团体叫做Red Team。

“RED TEAM“ (红队)， 涵盖的范围甚广(传统的渗透测试，属于其中的一种具体实现)。
意思形态上，是一种对抗的抽象。

# 红队和渗透测试？

**在时间上：**

红队的一个生命周期为数周或更久，比较灵活且无固定时间限制

渗透测试为几天一周左右，需要指定目标范围和测试时间；

**在深度上：**

红队可以进行深入的后渗透，社会工程学等等贴近真实攻击的手法，

国内的渗透测试还是以发现漏洞为主，一般情况下不可以进行后渗透等等。

**在实施过程上：**

红队注重测试的隐蔽性，尽可能的绕过现有的防御系统，拿到目标权限。

渗透测试一般会提前告知防御团队且设置白名单无需隐藏测试行为，有限的时间内尽可能地发现更多漏洞；

# 什么是C2？

C&C服务器的全称是Command and Control Server，

即“命令及控制服务器”

在红队行动中常用的C2服务有CS等等

# 为什么需要红队基础设施？

想象一下，我们正在进行红队行动。
竭尽全力甚至卖了身钓鱼了个运营姐姐或者绕过了迷人热情的WAF
最终获得了一个激动人心内网通向的shell。
我们高兴得像个孩子。
去抽支华子，准备一套乱入
但是。。。。。卧槽，shell怎么没了
卧槽，C2也没了
卧槽。。。。

这就十分快乐

# 为什么需要红队基础设施？

但是从蓝队的角度来看，她们注意到流量流向未知域。
像小BB那样好奇的打开他们的浏览器并访问到该站点。404错误。

怀疑让++了。
五分钟后，我们的SHEll变得无响应。
甚至一个ip段都没了

合理的**红队基础设施**可以使我们隐藏C2和流量
也可以使我们快速建立新的SHEll
也能使我们快速建立起新的体系

# 红队基础架构

工欲善其事，必先利其器。一次成功的红队行动是离不开强有力的基础架构的支持的。

**红队基础架构要注意：**

稳定性

总体系统稳定性能以及可靠的通信通道和访问通道。

安全性

尽量隐藏C2,流量等等以防止蓝队的朔源，反制等等。

扩展性

根据团队和行动要求添加/删除/修改功能。

# RedTeam基础架构

**红队基础架构要实现的功能：**

**隔离**

所有C2和不同功能的应按功能隔离

**重定向器**

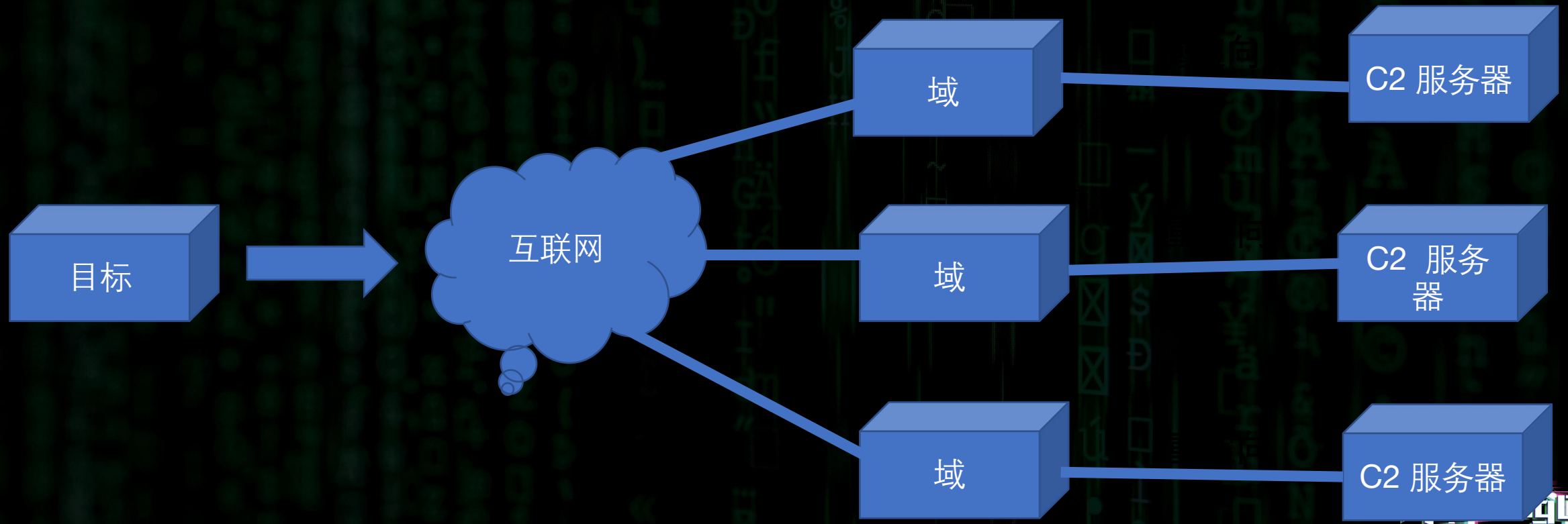
在每个后端服务器前使用某种重定向器。重定向器为我们的后端团队服务器提供了掩护

**隐藏**

不要让蓝方发现

# RedTeam基础架构

一个典型的红队攻击基础设施



# RedTeam基础架构

上面的基础设施很常见。
缺点有很明显

缺点：功能未分离、回连日志多、灵活性较低
也没有任何的措施来防止蓝队的反制

那么。。。。

# 红队基础架构

当我们需要长期（数周，数月，数年）的红队基础架构时，
根据功能隔离每种资产非常重要。

当蓝队开始检测到我们的活动时，一个合理的架构可以提供了弹性和敏捷性。

例如，如果蓝队识别出评估的网络钓鱼电子邮件，则红队将只需要创建一个新的SMTP服务器和有效负载托管服务器，而不是整个团队服务器的设置。

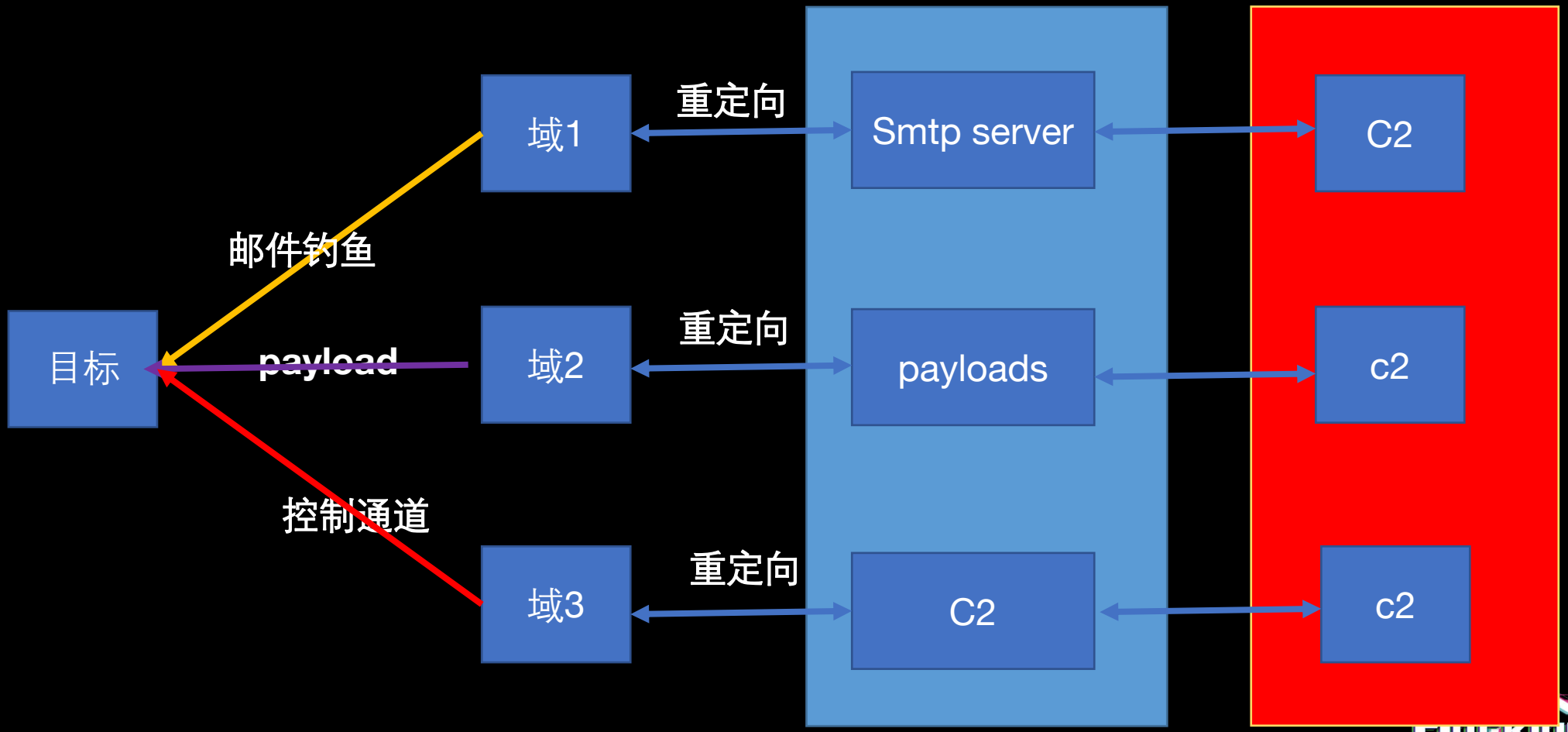
# 红队基础架构

那么我们考虑将这些功能划分到不同的资产上：

网络钓鱼SMTP
网络钓鱼有效载荷
长期指挥与控制（C2）
短期控制C2

每个红队行动都可能需要这些功能中的每一个，
也可以快速扩展所需的功能

# 红队基础架构


域1
重定向
Smtp server
C2
邮件钓鱼
目标
payload
域2
重定向
payloads
c2
控制通道
域3
重定向
C2
c2

# Tips1：域

从实战中我们都知道

一个高信誉的域名或一个具有迷惑性的域名对红队行动的帮助非常大

那么我们可以从两方面入手：

# Tips1：域

1.抢注过期域名，这样就可以继承该域名的信誉值
优先抢注与目标具有迷惑性的域名，这里要注意隐藏下**注册信息**

还有要**注意选择的域不能与任何先前的恶意软件或网络钓鱼活动相关联**
**这个可以去VT、微步检查，域名是否被标黑**

域名查找抢注网站
http://expireddomains.net
https://www.domcop.com/
https://www.freshdrop.com/

# Tips1：域

2.培养域名，购买与目标具有相似性的域名

对域名进行“养号”

例如主动提供到分类网站上，把域名解析到大公司ip上
使用的时候解析到C2不用解析回大公司

# Tips1：域

在这个Tips中最重要是

考虑因素是找到一个与目标环境与目标具有迷惑性的域名域。

通常，我们可以优先选择包括近似目标域名的域名，

例如：360.com的36o.com

与常见服务相似的域名（例如微信，Microsoft）或通用的行业域名。

# Tips2：有效负载重定向

有效载荷重定向器应在我们的木马回连前配置好。

Web重定向器分为两个主要类别：

# Tips2：有效负载重定向

## 1.socat和iptables：

接收在一个端口上接收的流量并将其全部地代理转发到另一个IP和/或端口。默认情况下，这些重定向器提供有限的日志记录，从而降低了监控流量的能力。

# Tips2：有效负载重定向

## 2.过滤重定向器（即Apache mod_rewrite和nginx）

允许基于请求中的不同属性（例如请求URI或用户属性）来处理每个请求。
这些重定向器提供了一些方法，可以对的后端基础结构进行一些非常复杂的处理。

过滤重定向器通常是更好的选择，但是它们的配置时间较长。

：

# Tips2：有效负载重定向

使用重定向器主机，

仅允许命令和控制（C2）流量到达我们的Cobalt Strike服务器，

并将所有其他流量重定向到无害的网站

：

# Tips2：有效负载重定向

好处是，如果我们的域被拦住，
我们真正的Cobalt Strike团队服务器的IP仍将可用。

我们可以更新重定向器，获取新的IP和域，然后恢复正常运行。

如果我们在信标有效负载中设置了多个回调域，
则甚至不需要重新获得初始访问权限。

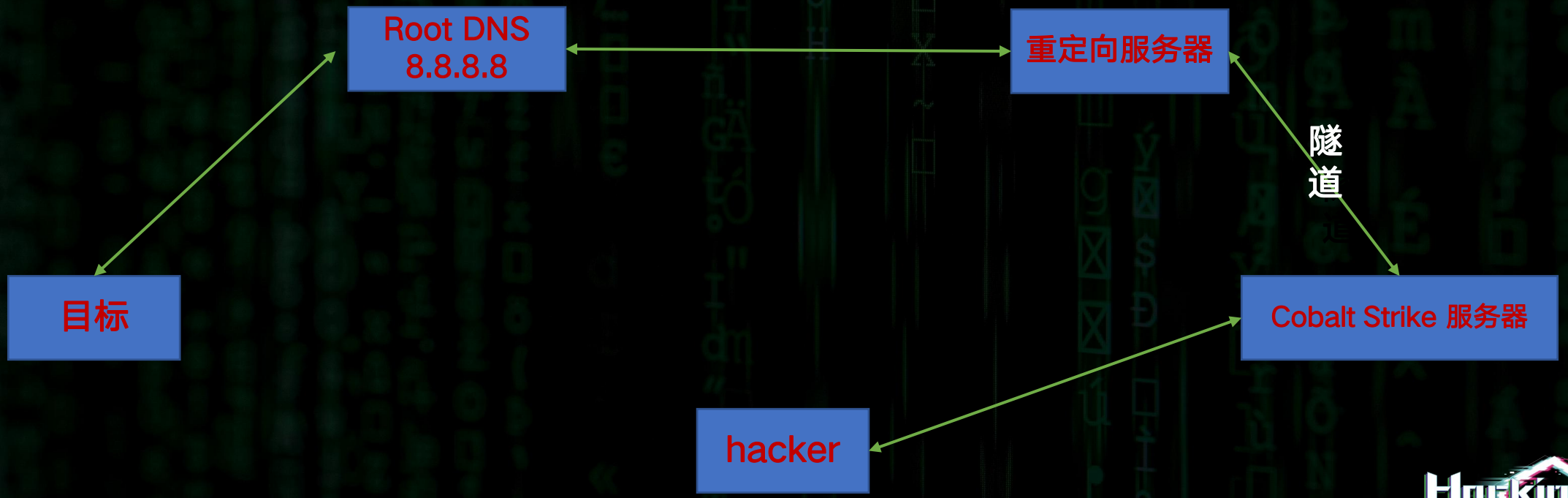
:

# Tips2：有效负载重定向

重定向Cobalt Strike DNS

首先，我们需要有一台运行Cobalt Strike团队服务器的服务器
和一台作为重定向运行的服务器。
可以参考以下：

# Tips2：有效负载重定向



# Tips2：有效负载重定向

Tips：

Cobalt Strike团队服务器与重定向服务器放在完全不同的IP段上
即使重定向服务器让蓝队反制溯源封IP了，也不会不仅会阻止我们CS的IP范围

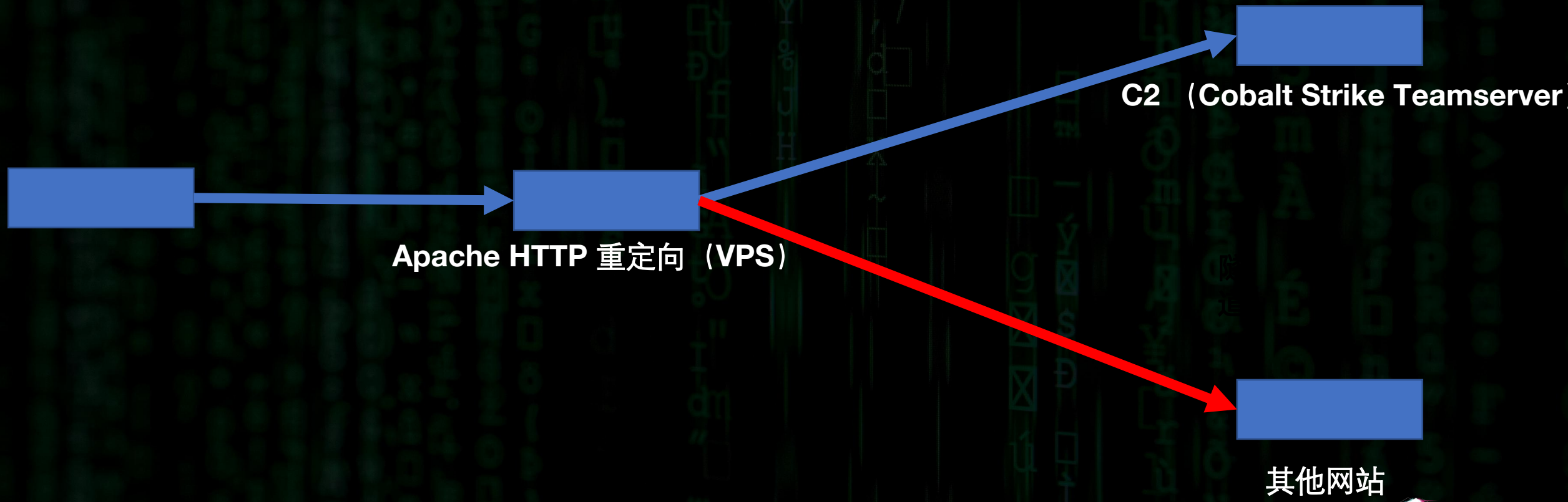
# Tips2：有效负载重定向

使用Apache mod_rewrite的Cobalt Strike HTTP C2重定向器

使用Apache重定向器作为中转服务器。
我们的C2域将指向Apache重定向器，它将执行流量过滤

例如：仅允许命令和控制（C2）流量到达我们的Cobalt Strike服务器，
并将所有其他流量重定向到无害的网站

# Tips2：有效负载重定向




主机将接收和发送Beacon使用的所有流量，并将其发送回（发送给Cobalt Strike团队服务器）

# Tips3：访问控制选项

不一定是蓝方才需要访问控制

有效的访问控制选项包括基于IP或指纹的重定向，有效载荷链接到期以及无效的URI重定向。

建议使用多个判断过来请求，拒绝使用默认uri，用来对抗安全厂商全网C2扫描

仅允许目标相关IP访问，对抗云沙盒检测

权限最小化

记录完整日志

设置告警

日志中心

# Tips4：C2

我们在上面说了我们的两种C2.短时间控制C2和长时间控制C2

**长时间控制C2**仅应用于长时间控制和重新获得对环境的访问。
服务器应从持久性接收回连，并非常缓慢地接收数据，例如每十二小时一次接收。

# Tips4：C2

短时间控制C2是用于所有主要操作的服务器。

将用于频繁与目标进行交互，发送命令和接收获取的数据。

考虑在目标环境的不同部分中使用具有更多安全控制措施的不同的短途服务器。

# Tips5：使用C2的协议

我们要选择使用的C2协议可能是红队基础架构的最重要方面了

最常见的C2协议是HTTP（S），DNS，域前沿和流行的第三方服务上的C2。

每个协议都有其自身的优点和缺点，并且它们相关的检测功能通常会有所不同。我们可以通过执行各种操作，观察延迟和压力测试，来挑选我们在红队行动使用的C2协议（带有重定向器）。

# Tips5：使用C2的协议

下图列出了常见C2协议的一些优点和缺点：**仅供参考**

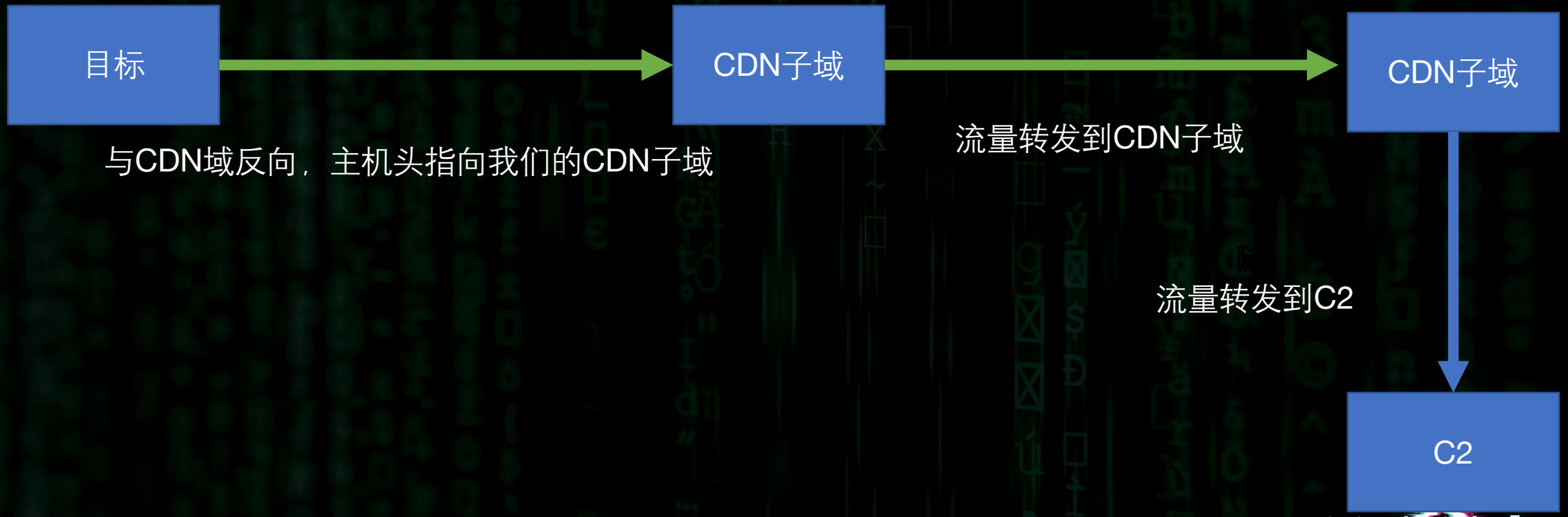
| 属性 | Http（s） | DNS | 域前置 | 第三方C2 |
| --- | --- | --- | --- | --- |
| 潜伏性 | 低 | 高 | 中 | 中 |
| 可检测性性 | 中 | 高 | 低 | 低 |
| 使用难度 | 低 | 低 | 中 | 中 |
| 可扩展性 | 低 | 低 | 中 | 中 |

# Tips5：使用C2的协议

## Tips5：使用C2的协议-域前沿

域前沿是用通过合法且高度信任的域路由流量逃避审查制度服务和应用程序检测使用的一种技术。
简而言之，流量通信过程使用受信任服务提供商的DNS和SNI名称，
当服务器接收到流量后，数据包将转发到数据包的主机标头中指定的原始服务器。
不同服务提供商有不同的转发方法，

# Tips5：使用C2的协议



# Tips6：第三方服务C2

允许第三方程序充当Cobalt Strike的Beacon有效载荷的通信层。

这些第三方程序连接到Cobalt Strike，以读取目标帧，并使用以这种方式控制的有效负载的输出来写入帧。

这些第三方程序使用外部C2服务器与Cobalt Strike团队服务器进行交互。

**例如：**

Office365、Pastebin、Slack、Facebook、Dropbox、Gmail、Twitter.

# Tips7：自动化部署

自动化可用于大大减少部署时间
从而使红队可以在更短的时间内部署更复杂的设置。

# 扩展阅读

https://awesomeopensource.com/project/bluscreenofjeff/Red-Team-Infrastructure-Wiki#domain-fronting

Red Team Infrastructure Wiki
A Vision for Distributed Red Team Operations - Raphael Mudge (@armitagehacker)
Infrastructure for Ongoing Red Team Operations - Raphael Mudge
Advanced Threat Tactics (2 of 9): Infrastructure - Raphael Mudge
Cloud-based Redirectors for Distributed Hacking - Raphael Mudge
6 Red Team Infrastructure Tips - Alex Rymdeko-Harvey (@killswitch-gui)
How to Build a C2 Infrastructure with Digital Ocean – Part 1 - Lee Kagan (@invokethreatguy)


HackingLab
技术队
感谢聆听