【译】一套可用于强化红队基础设施的补充资源

章鱼小团子 / 2017-06-06 23:42:00 / 浏览数 6518 技术文章 企业安全 顶(0) 踩(0)

本文旨在提供一套红队可安装的基础设施资源。 是为了补充Steve Borosh (@424f424f) 和Jeff Dimmock (@bluscreenofjeff)在BSides NoVa 2017的演讲："Doomsday Preppers：强化你的红队基础设施" (幻灯片)

原文链接

目录

设计注意事项

功能隔离

在设计一个稳定可用的长期红队基础设施时（范围为星期，月，年），根据功能分隔每个资产就很重要。当攻防所用资产被检测到时，这将为蓝队提供弹性和灵活性。例如，

考虑将这些功能分为不同的资产：

- 网络钓鱼SMTP
- 网络钓鱼payloads
- 长期命令控制（command and control，即C2）
- 短期C2

每个社会工程活动都可能需要这些功能。由于事件积极响应是红队评估中的典型要求，所以每个攻防比赛都应该实施一套新的基础设施。

使用重定向器

为了增进基础设施的恢复力和隐蔽性，每个后端资产（即，teamserver）应该在前端部署一个重定向器。目标是使我们的目标和后台服务器之间始终存在一个主机。以这种方
无需启用新的teamserver、迁移会话，或在后端重新连接未刻录的资产。

常用重定向器类型：

- SMTP
- Payloads
- 网络流量
- C2（HTTP（S），DNS等）

每个重定向器类型都有多个执行选项，适合不同的场景。这些选项将在本文的重定向器部分进一步详细讨论。重定向器可以是VPS主机，专用服务器，甚至可以在PaaS上运行

示例设计

这是一个示例设计，保持功能隔离并使用重定向器：

其他资源

> 分布式红队运作愿景 - Raphael Mudge (@armitagehacker)
>
> 持续红队运作的基础设施 - Raphael Mudge
>
> 高级威胁策略(2-9)：基础设施 - Raphael Mudge - Raphael Mudge
>
> 用于分布式黑客攻击的基于云的重定向器 - Raphael Mudge
>
> 6红队基础设施技巧 - Alex Rymdeko-Harvey (@killswitch-gui)

域名

根据您的目标使用的产品及其配置，域名的声誉会有很大差异。因此，选择一个适用于您的目标的域名不是像科学般有精确答案。开放源码情报收集（OSINT）对于帮助猜测

expireddomains.net 是最近过期或丢弃的域名的搜索引擎。它提供搜索和高级过滤，如过期年龄，反向链接数，Archive.org快照数， SimilarWeb
分数。使用该网站，我们可以注册之前使用过的域名，这些域名看起来与我们的目标或模拟对象相似，或者可能简单地混入我们的目标网络。

选择C2或数据渗漏的域名时，请考虑选择一个分类为金融（Finance）或医疗（Healthcare）的域名。由于可能出现法律或数据敏感性问题，许多组织不会对这些类别执行S

工具CatMyFish由Charles
Hamilton制作(@MrUn1k0d3r)，可以自动搜索并与expireddomains.net和BlueCoat进行分类Web检查。它可以被修改为对搜索开启更多的过滤器，甚至对您注册的资产进

另一个工具, DomainHunter 由Joe Vest (@joevest)和 Andrew Chiles (@andrewchiles)制作,建立在CatMyFish所做的并且返回BlueCoat和IBM
X-Force分类，域龄，备用的可用TLD，Archive.org链接和HTML报告。查看有关该工具发行的博客文章了解更多详细信息。
最后，确保您的DNS设置已正确传递。

- DNS checker

分类和黑名单检查资源

- McAfee
- Fortiguard
- Symantec + BlueCoat
- SenderBase数据库
- MultiBL
- MXToolBox - 黑名单

网络钓鱼设置

简单的基于Web的网络钓鱼

网络钓鱼从来都不是一件简单的事。建立适当的网络钓鱼基础设施可能会非常痛苦。以下教程将为您提供知识和工具，以快速搭建一套可绕过"大多数"垃圾邮件过滤器的网络

一旦您有一个域名通过上一节中列出的正确检查，并将您的网络钓鱼服务器组建好，您需要为您的域名创建一个"A"记录，如图所示。

接下来，ssh进入您的网络钓鱼服务器，并下载以下脚本来设置您的基础架构的上半部分。
Postfix-Server-Setup-Script
将脚本设置为可执行文件，如"chmod + x
ServerSetup.sh"。现在我们可以运行安装脚本，并通过选择任一选项来准备Debian或Ubuntu镜像，安装正确的依赖关系，并设置主机名来开始安装。

服务器将重启。SSH回到服务器并再次运行脚本。这次，选择选项4安装LetsEncrypt证书。确保你的A记录设置和传送正常。按照提示，您应该收到一条消息，通知您证书已

接下来，我们按照脚本选项5设置邮件服务器。再次按照提示操作，你将设置一个可运行的邮件服务器。现在，依照脚本选项7获取需要添加到DNS记录的DNS条目。提示：

您已经完成了第1部分。接下来，您将通过简单的步骤安装网络钓鱼Web前端。首先将最新版本的iRedMail
下载到您的钓鱼Server。简单的方法是右键单击下载按钮，复制链接地址，使用wget直接下载到您的钓鱼Server上。接下来，打开它。您可能需要安装bzip2归档程序。导航
+ x iRedMail.sh ）。以root身份执行脚本，按照提示操作，并登录到iRedMail服务器面板！

现在，创建一个用户进行网络钓鱼。

使用您的新用户登录到RoundCube界面，开始网络钓鱼！

重定向器

SMTP

“重定向器”可能不是描述我们所要完成工作最好的单词，但其目标与我们的其他重定向器相同。我们希望从最终的邮件头删除我们的网络钓鱼踪迹，并在受害者和后端服务器

我们要配置SMTP重定向执行以下两个关键操作：

发送邮件

删除之前的服务器头

将以下行添加到 `/etc/mail/sendmail.mc`:

```
define(`confRECEIVED_HEADER&#39;,`by $j ($v/$Z)$?r with $r$. id $i; $b&#39;)dnl
```

添加到`/etc/mail/access`末尾:

```
IP-to-TeamServer *TAB* RELAY
Phish-Domain *TAB* RELAY
```

从收件人的电子邮件头中删除发件人的IP地址

从邮件服务器设置中删除头信息

配置全部地址

This will relay any email received to *@phishdomain.com to a chosen email address. This is highly useful to receive any responses or bounce-backs to a phishing email.

这将会将收到的任何电子邮件转发到*@phishdomain.com到所选的电子邮件地址。这是非常有用的接收任何回应或反弹到网络钓鱼电子邮件。

```
echo PHISH-DOMAIN &gt;&gt; /etc/mail/local-host-names
```

`/etc/mail/sendmail.mc`文件中，在以下行`//Mailer Definitions//`之前增加:

```
FEATURE(`virtusertable&#39;, `hash -o /etc/mail/virtusertable.db&#39;)dnl
```

将以下行添加到 `/etc/mail/virtusertable`:

```
@phishdomain.com  external-relay-address
```

注意：这两个字段应该是tab分隔的

Postfix

Postfix是一个更容易并具有更广泛兼容性的sendmail的替代品。Postfix还提供完整的有Dovecot的IMAP支持。这样，测试人员就可以实时跟踪回应了原始邮件的网络钓鱼

Julian Catrambone(@n0pe_sled)发表的Mail Servers Made Easy提供了一个完整的针对网络钓鱼设置Postfix邮件服务器的指南。

DNS

socat

socat可用于将端口53上的传入DNS数据包重定向到我们的团队服务器。虽然此方法有效，但有些用户已经报告了使用此方法时Cobalt
Strike存在延迟问题。4/21/2017编辑：以下socat命令似乎可以解决问题，由测试员@xorrior提供：

```
socat udp4-recvfrom:53,reuseaddr,fork udp4-sendto:<IPADDRESS>; echo -ne
```

重定向Cobalt Strike DNS信号 - Steve Borosh

iptables

iptables DNS转发规则与Cobalt Strike一起运行良好。似乎没有任何socat处理这种类型的流量的问题。

以下是DNS重定向器规则集的示例。

```
iptables -I INPUT -p udp -m udp --dport 53 -j ACCEPT
iptables -t nat -A PREROUTING -p udp --dport 53 -j DNAT --to-destination ip:53
iptables -t nat -A POSTROUTING -j MASQUERADE
sysctl net.ipv4.ip_forward=1
```

另外，将“FORWARD”链策略改为“ACCEPT”

DNS重定向也可以在NAT之后完成

有时可能需要在内部网络上托管c2服务器。使用IPTABLES，SOCAT和反向ssh隧道的组合，可以通过以下方式来实现。

在这种情况下，我们的volitile重定向器使用本节前面描述的规则，用IPTables转发所有DNS流量。接下来，我们从我们的内部c2服务器到我们的主要重定向器创建一个SSH
server上启动socat，将6667端口上的任何传入TCP流量分配到UDP端口53，DNS
c2需要监听。最后，我们类似地在主重定向器上设置一个socat实例，以将任何传入53端口的UDP流量重定向到端口6667的SSH隧道。

HTTP(S)

socat与mod_rewrite对比

socat提供了重定向功能。任何在socat指定的源接口/端口上接收到的请求都将重定向到目标IP /端口。无过滤或条件重定向。另一方面，Apache
mod_rewrite提供了多种方法来加强网络钓鱼，并提高测试基础架构的弹性。mod_rewrite可以根据请求属性（如URI，用户代理，查询字符串，操作系统和IP）执行条件重
mod_rewrite使用htaccess文件配置规则集，控制Apache应如何处理每个传入的请求。使用这些规则，例如，您可以使用默认的wget
UA将到您的服务器的请求重定向到目标网站的合法页面。

简而言之，如果重定向器需要执行条件重定向或高级过滤，请使用Apache mod_rewrite。否则，使用可选iptables过滤的socat重定向就足够了。

Payloads和Web重定向

在提供payload和网络资源时，无论是建立C2还是收集情报，我们都希望尽量弱化事件响应者查看文件的能力，并增加成功执行有效载荷的机会。

Apache ModRewrite的用法和示例：Jeff Dimmock：

- 使用Apache mod_rewrite加强您的网络钓鱼
- 使用Apache mod_rewrite的无效的URI重定向
- 基于操作系统的重定向与Apache mod_rewrite
- 使用Apache mod_rewrite的事件响应
- 使用Apache RewriteMap的过期钓鱼链接
- Apache mod_rewrite Grab Bag

要在重定向服务器上自动设置Apache Mod_Rewrite，请查看Julain Catrambone(@n0pe_sled)博客文章 Mod_Rewrite Automatic Setup及其附带的工具

C2 重定向器

重定向C2流量有双重意图：模糊后端team服务器，以及如果事件响应者浏览网页，可看到似乎是合法的网站。通过使用Apache
mod_rewrite和定制的C2配置文件或其他代理（例如使用Flask），我们可以可靠地过滤来自调查流量中的真实C2流量。

- Cobalt Strike HTTP C2 Redirectors with Apache mod_rewrite - Jeff Dimmock
- Expand Your Horizon Red Team – Modern SAAS C2 - Alex Rymdeko-Harvey (@killswitch-gui)

其他 Apache mod_rewrite 资源

- mod-rewrite-cheatsheet.com
- Official Apache 2.4 mod_rewrite Documentation
- Apache mod_rewrite Introduction
- An In-Depth Guide to mod_rewrite for Apache
- Mod_Rewrite/.htaccess Syntax Checker

修改C2流量

Cobalt Strike

Cobalt Strike通过Malleable C2配置文件修改其通信流量。配置文件提供了高度可定制的选项，用于修改服务器的C2流量如何在链路上显示。Malleable C2配置文件可用于加强躲避事件响应==incident response evasion==，模拟已知对手或伪装成目标使用的合法内部应用程序。

- Malleable C2 Profiles - GitHub
- Malleable Command and Control Documentation - cobaltstrike.com
- Cobalt Strike 2.0 - Malleable Command and Control - Raphael Mudge
- Cobalt Strike 3.6 - A Path for Privilege Escalation - Raphael Mudge
- A Brave New World: Malleable C2 - Will Schroeder (@harmj0y)
- How to Write Malleable C2 Profiles for Cobalt Strike - Jeff Dimmock

Empire

Empire使用通信配置文件，它为GET请求URI，UA和请求头提供定制选项。配置文件由各元素组成，由管道字符分隔，在`listeners`菜单中的`set DefaultProfile` 选项进行设置。

以下是默认配置文件示例：

```
&quot;/CWoNaJLBo/VTNeWw11212/|Mozilla/4.0 (compatible; MSIE 6.0;Windows NT 5.1)|Accept:image/gif, image/x-xbitmap, image/jpeg,
```

或者，DefaultProfile值可以在Empire初始设置之前通过修改`/setup/setup_database.py`文件来设置。这将更改Empire使用的默认通信配置文件。

- Default Empire Communication Profiles (in Empire GitHub repo)
- How to Make Communication Profiles for Empire - Jeff Dimmock

Domain Fronting

Domain Fronting通过合法和高度信任的域来路由流量，用于逃避技术检测。支持Domain Fronting 的流行服务包括Google App Engine, Amazon CloudFront, 和Microsoft
Azure。简而言之，流量使用可信服务提供商的DNS和SNI名称，下面的示例中使用了Google。当边缘服务器接收到流量（例如：位于gmail.com）时，数据包将转发到数
Server（例如：phish.appspot.com）。根据服务提供商，Origin
Server将直接将流量转发到指定的域（我们将指向我们的teamserver），或者需要代理应用程序来执行最后一跳。

有关Domain Fronting如何工作的更多详细信息，请参阅白皮书通过domain fronting阻止通信和TOR项目的文档

寻找潜在的Frontable Domains的有用工具

- FindFrontableDomains

其他资源

- High-reputation Redirectors and Domain Fronting - Raphael Mudge
- Empire Domain Fronting Chris Ross (@xorrior)
- Domain Fronting via Cloudfront Alternate Domains - Vincenty Yiu (@vysecurity)
- Escape and Evasion Egressing Restricted Networks - Tom Steele (@_tomsteele) and Chris Patten

基础安全配置

攻击基础设施与任何其他互联网连接的主机相同，都可能受到攻击，同时，由于正在使用的数据和到目标环境的连接，攻击基础设施应被认定为高度敏感的。

在2016年，最常见的攻击工具被披露存在远程代码执行漏洞：

- 2016 Metasploit RCE Static Key Deserialization
- 2017 Metasploit Meterpreter Dir Traversal Bugs
- Empire Fails - Will Schroeder
- Cobalt Strike 3.5.1 Important Security Update - Raphael Mudge

应该使用iptables来过滤不需要的流量并限制所需基础设施元素之间的流量。例如，如果Cobalt
Strike服务器仅向Apache重定向器提供资产，则iptables规则应仅允许来自重定向器的源IP的端口80。这对于任何管理界面（例如SSH或Cobalt
Strike的默认端口50050）尤其重要。此外还可以考虑阻止非目标国家/地区的IP。

chattr可以用于teamserver，以防止修改cron目录。使用chattr，您可以限制任何用户（包括root）修改文件，直到删除chattr属性。

SSH应该仅限于公钥身份认证，并配置为使用受限权限用户进行初始登录。为了增加安全性，请考虑向SSH添加多因素认证。

更新！没有提醒定期更新系统，并根据需要执行热修复来修复漏洞的安全列表都不完整。

当然，这个列表并不是teamserver的全部安全措施。基础设施的常见安全措施：

- Red Hat Enterprise Linux 6 Security Guide
- Debian Documentation on Hardening
- Securing Debian Manual
- 20 Linux Server Hardening Security Tips - nixCraft
- SANS Linux Security Checklists

提示

- 记录一切 - 运行一套复杂的红队基础设施意味着许多更改的部分。确保记录每个资产的功能和流量发送的目的地。

  在不同服务提供商和区域之间划分资产 -
  基础设施资产应分散在多个服务提供商和地理区域。蓝队成员可能针对被识别为主动攻击的服务商来源提高监视阈值，甚至可能彻底阻止该服务提供商。注意：如果跨越

  监控日志 -
  应在整个交互过程中进行所有日志监控：SMTP日志，Apache日志，socat重定向器上的tcatdump，iptables日志（特指流量转发或有针对性的过滤），weblogs，Cob
  Strike / Empire /
  MSF日志。将日志转发到集中地，例如使用rsyslog，以便于监控。@Killswitch_GUI创建了一个名为lTerm的易用的程序，它将所有bash终端命令记录到集中地。用lTer

- 指纹事件响应 -
  如果可能，在评估开始之前尝试被动或主动指纹IR操作。例如，将普通的网络钓鱼电子邮件发送到目标（使用不相关的基础架构）并监视基础设施接收的流量。IR团队调

上一篇：【非原创】渗透测试标准 下一篇：漏洞修复方案汇总Book

1. 1 条回复


hades 2017-06-07 00:59:37

团子妹纸，辛苦了

0 回复Ta
