# kali-linux安装chrome浏览器,配置burpsuite完整教程



yink12138 于 2021-07-26 22:16:47 发布 6 1001 收藏 7 分类专栏: linux 文章标签: linux chrome bash 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>版权协议,转载请附上原文出处链接和本声明。 本文链接: https://blog.csdn.net/yink12138/article/details/118887795 版权

<u>linux 专栏收录该内容</u> 5 篇文章 0 订阅 订阅专栏

先说几句题外话,因为是刚刚开始发文章,看了一下前面发的几篇,感觉挺散的,其实我是搞CTF的web 菜鸡,然而一篇writeup都还没写...之后有时间写点writeup算了2333然后这篇文章呢本质上是我从windows向 linux迁移的血泪之路...的一小部分...实在没用过实在不习惯...但是作为CTFer,kali也算是必修课了。所谓:

Kali玩得好,监狱进的早。牢饭吃到老

就是这个道理。

另外,在kali联网方面也遇到了点问题,也是关于证书不信任的,有空写一篇...

Anyway,进入正题。

#### 1.安装chrome浏览器

本人比较喜欢用Chrome,拓展比较多,也有一定习惯原因。

具体安装步骤可以看这篇文章: 在 Kali Linux 中如何安装 Google Chrome | 《Linux就该这么学》 (linuxprobe.com)

在用命令行指令启动浏览器时有几点注意:

(1).如果用命令行启动浏览器,请不要关闭命令行,否则你的浏览器也会一起关闭。

(2).一定要用普通用户启动浏览器,不要用root用户,不要用root用户,不要用root用户! (重要的事情说三遍),root用户貌似不支持sandbox,可以参考这篇文章:Running as root without --no-sandbox is not supported\_qq\_41290048的博客-CSDN博客

### 2. 配置 burpsuite

如果你还没有在你的系统上安装burpsuite或者想安装专业版(kali自带的是社区版),我建议看这篇文 章: Kali 配置BurpSuite Professional 教程\_林英俊的博客-CSDN博客,这篇文章讲的很详细,但是如果你跟着 上面的教程做到了最后一步"设置快捷方式",不要着急,请先回来,看完下面的提示!

#### 提示:

(1)linux的命令行主要分为两种,zsh和bash(tcsh我不太了解)。上面的文章适用于正在使用bash命令行的朋友们,然而kali最新版的默认命令行是zsh类型...(其实zsh比bash要好用,有自动提示更正这些,但是好像很多linux设备上面默认命令行仍然是bash,不过建议用zsh)。所以,首先你要看看自己的命令行类型。

可以用这个命令: ps -p \$\$

我的显示结果:

PID	TTY	TIME	CMD
4872	pts/1	00:00:00	zsh

可以看到,最后一项就是你当前使用的shell类型,我的是zsh。

如果是zsh,请将配置文件从.bashrc改为.zshrc,其余的操作不变~

(2)vim文本编辑器小技巧:在浏览文件时,输入/,之后输入你要查找的内容,就能快速查找定位~点击a键可以将光标定位在当前位置进入浏览界面,Esc键可以退出编辑,浏览文件时输入:wq并回车可以保存并退出。 更多的vim指令参见这篇文章:Linux基本命令 vim命令(一)-lizhouwei-博客园 (cnblogs.com)

OK,相信到现在你应该在自己的系统上安装了burpsuite了,下面让我们看看Chrome上面如何配置代理。

首先,burpsuite需要配置证书。分成三步:

(1)设置burpsuite的端口

先打开burpsuite,设置监听端口。下方图片来自: kali笔记(七) burpsuite设置代理\_孤的博客-CSDN博客

Burp Indude: Beegeter Window Help Target Frow bide: Scanner Intruder: Repeater Sequence: Decoder Compare Extender Project options User options Alerts  Procy Listeners  Proxy Listeners  Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.  Add Running Interface Invisible Redirect Edit Proxy listener  Remove Each installation of Burp generates its own CA certificate that Proxy listeners  Proce use of SSL Invisible proxy support linvisible proxying (enable only if needed)  Proxy sets based on the following rules: Each installation of the following rules: Each invisible proxy support linvisible proxying (enable only if needed)  Proxy support invisible proxying (enable only if needed)  Proxy sets based on the following rules: Each invisible proxying (enable only if needed)  Proxy support invisible proxying (enable only if	В	urp Suite Community Edition v1.7.36 - Temporary Project	- • ×
Target       Traget	Burp Int <mark>ruder Repe</mark> ater Window Help		
Intercept Client Requests       Options         Import export CA certificate       Regenerate CA certificate         Import export CA certificate       Support invisible proxying (anable only if needed)	Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder	Comparer Extender Project options User options Alerts	
Proxy Listeners Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server. Add Running interface invisible Redirect Edit  Clintercept Client Requests Burp Proxy listeners Each installed for viewing and edition Intercept Client Requests are stalled for viewing and edition Intercept requests based on the following rules: Add Enabled Operator Match type: Relationship Add Enabled Operator Match type: Relationship	Intercept HTTP history WebSockets history Options		
Edit	Intercept       HTTP history       WebSockets history       Options         Proxy Listeners       Burp Proxy uses listeners to receive incoming HTTP requests from your browser         Add       Running       Interface       Invisible       Redirect         Add       Renning       Interface       Invisible       Redirect         Edit       Image: Comparison of Burp generates its own CA certificate that Proxy listeners c       Import / export CA certificate         Remove       Regenerate CA certificate       Regenerate CA certificate         Intercept Client Requests       Use these settings to control which requests are stalled for viewing and edition         Intercept requests based on the following rules:       Add         Enabled       Operator       Match type         Relationship       File extension       Does not match		of Burp.
	Remove And URL Is in target scope Up Down	OK Cancel	
Remove     And     URL     Is in target scope       Up     OK     Cancel	Automatically fix missing or superfluous new lines at end of request Automatically update Content-Length header when the request is edited	https://blog.c:	sdn.net/Wu00099

(2)给浏览器设置代理

最简单的方式就是直接在设置里面打开代理。

首先打开设置

<b>杀筑</b>	
关闭 Google Chrome 后继续运行后台应用	
使用硬件加速模式(如果可用)	-
打开您计算机的代理设置	
	https://blog.csdm.net/yink12138

在"高级"中找到"系统"里的"打开计算机的代理设置"

↓ ‡ 设置 × +			• _ • ×
← → C			☆ 😩 :
设置	Q、 在设置中搜索		
▲ 您与 Google	自定义字体	•	^ _
自 自动填充	网页缩放	100% 👻	
<ul> <li>♡ 安全检查</li> <li>◎ 隐私设置和安全性</li> </ul>	搜索引擎		
🏶 外现	地址栏中使用的搜索引擎了解详情	Google 👻	
Q, 搜索引擎	管理搜索引擎	•	
<ul> <li>試入測览器</li> <li>① 启动时</li> </ul>	默认浏览器		
高级	Google Chrome 是您的默认浏览器		
扩展程序	启动时		
关于 Chrome	◎ 打开新标签页		
	○ 继续浏览上次打开的网页		
	〇 打开特定网页或一组网页		
	高级 ~		<b>(</b> ⊕ °, <b>)                                  </b>

打开下方的"高级"。

エルキ

🔽 | 🔲 🖻 🍃 🤀 🛄 ~ | 💽 🧿 21:45 拼 🗖 🔲 🏮 新标签页 - Google Chro. 🐻 Burp Suite Professional ... 🍙 qterminal ▣ 文件系统 🌲 🕑 | 🖴 G • \_ • × ☆ 😫 🗄 打开新的标签页 打开新的窗口 打开新的无痕式窗口 下载内容 Google 投射... 查找... 更多工具 Q 在 Google 上搜索,或者输入一个网址 Ļ 设置 帮助 \* (+) 百度一下,你... Chrome 网上.. 添加快捷方式 Burp Suite Pr. 中 % ) 11 至虚拟机内部单击或按 Ctrl+G。

点击打开,然后在里面进行设置即可。

一般来说上面的方法就够了,但是如果你遇到了和我一样的问题:

在受支持的桌面环境中运行Google Chrome时,将使用系统代理设置。但您的系统不受支持,或启动系统配置时出现问题。

但您仍可通过命令行进行配置。如需详细了解各项实验功能和环境变量, 请参见 man google-chrome。

还有第二种方法:

以普通用户的身份在命令行中运行命令: google-chrome --proxy-server="127.0.0.1:8080"

小技巧:可以利用alias自定义快捷命令,具体参考: Kali Linux基础操作学习篇——alias命令 - 知乎 (zhihu.com)(但是请同样注意bash与zsh的区别!)

这样配置代理就成功啦~

(3) 配置证书信任

首先下载证书,参见kali笔记(七)burpsuite设置代理\_孤的博客-CSDN博客

然后配置信任;

打开设置



打开左边的"隐私设置与安全性"选项卡。

设置	i i	Q、 在设置中搜索	
<u>.</u>	您与 Google	您与 Google	
Ê	自动填充		
۲	安全检查		
V	隐私设置和安全性		
<b>@</b> Q	外观 搜索引擎	在 Chrome 中畅享 Google 的智能技术在您的所有设备上同步并个性化设置 Chrome 开启同步环	力能
	默认浏览器	同步功能和 Google 服务	•
Ċ	启动时	自定义您的 Chrome 个人资料	•
高级	*	导入书签和设置	•
扩展 关于	程序 IZ	自动填充	
		<b>0</b> 密码	•
		☐ 付款方式	•
		♥ 地址和其他信息	•
		安全检查	
		Chrome 有助于保护您免受数据泄露、不良扩展程序等问题的影响 立即	检查

# 打开"安全"选项。

设置	Q、 在设置中搜索	
▲ 您与 Google	隐私设置和安全性	
<ul> <li>自动填充</li> <li>② 安全检查</li> </ul>	■ 清除減気数据 清除減気记录、Cookie、緩存及其他数据	•
<ul> <li>隐私设置和安全性</li> <li>A 30</li> </ul>	Cookie 及其他网站数据           已阻止无痕模式下的第三方 Cookie	•
<ul> <li>大水</li> <li>Q 搜索引擎</li> </ul>	安全     受	•
<ul> <li>試认浏览器</li> <li>() 启动时</li> </ul>	开      对      开      开      开      的      的      的      可      以使用和显示什么信息(如位置信息、摄像头、弹出式窗口及其他)	×
高級	▲ 隐私沙盒 试用版助能已开启	Z
扩展程序 🖸	外观	
	主题育录 GTK+	使用经典主题背景
	显示"主页"按钮 已停用	
	显示书签栏	
	使用系统标题栏和边框	
	字号 中(推荐)	*

打开"管理证书"选项。

设置	Q, 在设置中搜索	
② 您与 Google       自动填充       ② 安全检查       ② 陽私设置和安全性       ④ 外現       ④ 外現       ④ 規索引擎       □ 默认道览器       ① 启动时	<ul> <li>☆ 检测危险事件并在此类事件发生时向您发出警告</li> <li>1. 将网处与存储在 Chrome 中的不安全网站列表进行比对,如果某个网站企图窃取您的密码,或者您下我了有害的文件,Chrome 可能还会将相应网站连网少量网页内容发送给安全对发功能。</li> <li>第0款创为所有人改善网络农全环规 向 Google 发送您的问的部分网页的网址、有限的系统信息以及部分网页内容,以协助我们发现</li> <li>第1年初9月的大学的公式。</li> <li>第1年初9月的大学的公式。</li> <li>第1年初9月的大学校会会任何人员/任何一方(包括 Google)读取、</li> <li>第1年間</li> </ul>	
扩展程序 🖸 关于 Chrome	小会性非地及变更周期端。下就均容相当 麻性护的设备。在 Ginali 和i Google 推杀等承债 Google 直杀中, 者安全测说保护可用,您仍将获得该保护。           高级           管理交合密钥 重直安全密切并创建 PIN 码         ,           管理证书         ,           管理 HTTPS/SSL 证书和设置         ,           Google 高级保护计划 为所有可能会通到定向攻击的个人 Google 核号提供保护         [2]	
至虚拟机内部单击或按 Ctrl+G。		https://blog.csdn.net/yink12138

## 在里面选中"授权机构"选项卡。

设置		Q, 在设置中搜索	
💄 悠与 Google		← 管理证书	
自 自动填充			17 AL
🕏 安全检查			其他
😯 隐私设置和安全	è性	您有证书可标识以下证书授权中心	导入
🌳 外观			
Q, 搜索引擎		org-AC Camerfirma S.A.	~
默认浏览器		org-AC Camerfirma SA CIF A82743287	~
① 启动时		org-ACCV	~
高级	*	ord-Actalis S.p.A./03358520967	~
④ 语言			
		org-AffirmTrust	~
★ 无障碍		org-Agencia Catalana de Certificacio (NIF Q-0801176-I)	~
▲ 系统		org-Amazon	~
<ul> <li>① 重置设置</li> </ul>		org-Atos	~
扩展程序		org-Autoridad de Certificacion Firmaprofesional CIF A62634068	~
关于 Chrome		org-Baltimore	~
		org-Buypass AS-983163327	~

点击"导入",将你刚刚下载的证书导入。

但是我遇到的问题是导入不了刚刚下载的证书...

如果你遇到了这种情况,请把证书的格式由.der改为.crt,这样就能成功导入!

(其实其他浏览器的导入证书要简单得多,只有Chrome稍显麻烦…)

按照上面的步骤完成,到这里,你应该可以正常地用burpsuite抓包啦!

写了很久哈,如果对你有帮助,还希望给这篇文章点个赞,我也是在学习中,都是自己的亲身经历, 希望得到大家的鼓励,我会很开心哒~先谢谢各位啦~

文章已迁移至博客:https://yinkstudio.xyz,之后文章大多在博客上更新,欢迎关注~

