攻防世界misc之Cephalopod

原创

胖虎很忙 于 2019-11-19 20:57:50 发布 822 收藏

分类专栏： 攻防世界 misc ctf 文章标签： 攻防世界misc之Cephalopod

本文链接：https://blog.csdn.net/weixin_43877387/article/details/103142339

 攻防世界 同时被 3 个专栏收录

5 篇文章 0 订阅

订阅专栏

 misc

3 篇文章 0 订阅

订阅专栏

 ctf

10 篇文章 0 订阅

订阅专栏

Cephalopod

【原理】

流量分析, 图片还原

【目的】

掌握数据包分析方法

【环境】

Linux

【工具】

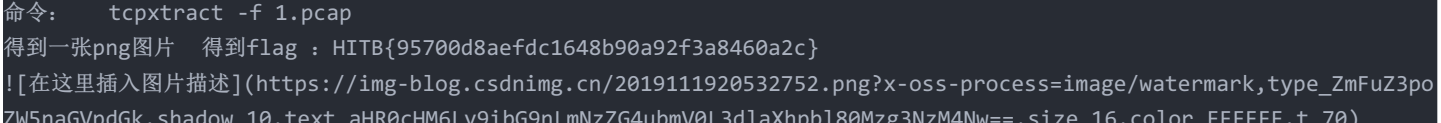
tcpxtract，binwalk

【步骤】

```
Step 1
```

首先用binwalk进行查看 ```bash $ binwalk 2a9c1cdd-2ac0-4b2a-828d-269c6e04ebbb.pcap

![在这里插入图片描述](https://img-blog.csdnimg.cn/20191119145354564.png)
Step 2

尝试使用foremost进行提取发现不可行，那么转换思路，使用其他工具进行提取，根据现有线索我们可以知道这是一个.pcap网络流量文件，所以可以尝试使用相关工具tcpxtract 进行提取
命令： tcpxtract -f 1.pcap
得到一张png图片 得到flag ：HITB{95700d8aefdc1648b90a92f3a8460a2c}

Step 3

Tcpxtract是一种基于文件签名从网络流量中提取文件的工具。基于文件类型的页眉和页脚（有时称为“雕刻”）提取文件是一种古老的数据恢复技术。Foremost这样的工具使用这种技术可以从任意数据流中恢复文件，其是专门用于通过网络传输的拦截文件的应用。填补类似需求的其他工具有流网和EtherPEG。driftnet和EtherPEG是用于在网络上监控和提取图形文件的工具，网络管理员通常使用它来警告用户的互联网活动。driftnet和EtherPEG的主要局限性在于它们只支持三种文件类型，不需要添加更多方法。他们使用的搜索技术也是不可扩展的，不会跨数据包边界搜索

```
bash $ tcpxtract -f 40150e85ac1b4952f1c35c2d9103d8a40c7bee55.pcap
Found file of type "png" in session [10.0.2.7:49818 -> 10.0.2.10:36890], exporting to 00000001.png Found file of
 type "png" in session [10.0.2.7:49818 -> 10.0.2.10:36890], exporting to 00000002.png 提取到flag
```

【总结】

在计算机网络管理中，pcap（packet capture）由捕获网络流量的应用程序编程接口（API）组成。类Unix的系统主要是在libpcap库中实现pcap，而Windows系统则是使用名为WinPcap的libpcap端口。

监控软件可能会使用libpcap或WinPcap捕获通过网络传播的数据包，并在较新版本中链路层的网络上传输数据包，以及获取可能与libpcap或WinPcap一起使用的网络接口列表。pcap API是用C编写的，所以其他语言，如Java，.NET语言以及脚本语言通常需要使用封装器，libpcap或WinPcap本身并不提供封装。而C++程序则可以直接链接到C API或使用面向对象的封装器。

libpcap和WinPcap提供了许多开源和商业网络工具的数据包捕获和过滤引擎，包括协议分析器（数据包嗅探器）、网络监视器、网络入侵检测系统、流量生成器和网络测试器。libpcap和WinPcap还支持将捕获的数据包保存到文件中，并读取包含保存的数据包的文件；使用libpcap或WinPcap可以编写应用程序，就能够很好的捕获网络流量并对其进行分析，或使用相同的分析代码读取保存的捕获并进行分析。以libpcap和WinPcap使用的格式保存的捕获文件可以由能够读取该格式的应用程序（如tcpdump，Wireshark，CA NetMaster或Microsoft Network Monitor 3.x）进行读取。

libpcap和WinPcap创建和读取的文件格式的MIME类型为application / vnd.tcpdump.pcap。典型的文件扩展名是.pcap，除此之外.cap和.dmp也是常用的。