Misc 总结 ----流量分析 场景模拟

M1n3 / 2018-01-22 22:32:24 / 浏览数 3461 安全技术 CTF 顶(0) 踩(0)

这是misc系列的最后一篇文章了。这篇文章主要由三个场景构成。

网络协议—暴力破解

实验目的

掌握暴力破解流量的分析方法
学会利用wireshark的filter过滤出有价值的信息

实验环境

- 操作机：Windows XP
  - 实验工具：
    - Wireshark

实验内容

这是一些本地服务被暴力破解的流量。提交Flag格式flag{尝试登录的次数_服务正确的密码}，如尝试98次登录，第98次登陆成功，使用密码123456则flag为flag{98_123456

实验一

整体分析流量包

方法一 使用wireshark的统计功能

wireshark菜单栏提供了功能，协议分级。本流量包全是已经过滤好的FTP流量方便分析。统计 - 协议分析 ：

通过这个功能是可以快捷的分析出流量包的都有一些什么协议，以及各种协议的占比。

方法二 过滤器的应用

通过前面实验对于FTP协议的学习，我们知道当返回码是230的时候用户成功登录。

应用过滤器`ftp.response.code==230`:

然后在第一个数据包右键追踪TCP流：

可以知道登录用户名ubuntu，成功登陆的密码：swings666。

接下来查找暴力破解尝试登录的次数。暴力破解用户的密码，我们可以直接过滤客户端发送的ftp命令：pass，应用过滤器`ftp.request.command == "PASS"`：

然后通过 统计 - 捕获文件属性 - 统计，已显示：

可以获知一共进行了41此密码尝试。所以综上Flag为flag{41_swings666}

网络协议-端口扫描

实验目的

了解端口扫描的原理
分析端口扫描工具的具体操作
通过流量还原扫描的结果

实验环境

- 操作机：Windows XP
  - 实验工具：
    - Wireshark2.2
    - binwalk for windows

实验内容

这是一些黑客使用扫描工具对目标主机进行扫描的流量，请问目标主机开放了哪些端口？对80端口的扫描中，是否有得到可以访问的目录？(flag格式：flag{端口号_端口号_

实验一

先分析目标主机开放的端口。

方法 观察TCP流

- 操作步骤详解

使用wireshark载入scan.pcapng，得益于wireshark会给我们标记不同数据包的颜色，我们可以看到大量的由192.168.233.128发给192.168.233.131不同端口的TCP，SYN

直接跟着这些TCP数据包，往后面看：

可以看到，向21，22，80端口发送的SYN是成功建立了TCP连接的，意味着端口开放。

实验二

继续分析流量，查看扫描端口后做了什么。

方法一 观察HTTP流量

先大致浏览一下后面的流量包，我们可以直接应用过滤规则：http过滤http流量分析。

结合之前所讲，我们知道当http访问成功的时候，是会返回http状态码，"200，ok"的。我们目前分析的流量包HTTP数据不是很多，可以直接去看，查找。观察过滤出来的

注释

有两个方法可以应用过滤器，在大量的数据包中过滤出我们想要得到的东西：

1. 在分组详情中右键，应用过滤器。
1. 使用filter的表达式功能。

实验三

分析FTP和ssh操作

方法一 FTP操作

序号为2203及附近的FTP数据包，获取了FTP服务器的banner欢迎信息，然后尝试了采用TLS方式连接和匿名用户登录等操作。

方法二 SSH操作

获取到SSH的版本协议等信息：`SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.1`

综上，flag为：flag{21_22_80_NO}

网络协议-漏洞分析

实验目的

分析入侵者的行为
了解二进制漏洞利用形式

实验环境

- 操作机： Windows 7

实验工具

- wireshark 2.2.*

实验内容

分析入侵者如何拿到服务器权限

方法

- 操作步骤详解

过滤HTTP流量，可见192.168.233.128访问了192.168.233.133的80端口，并成功获取了页面。h页面文件大，可以提取出来，使用浏览器打开。

我们得知这是一个`Easy File Sharing Web Server`然后注意到HTTP流量异常之处：

此时应该还不明白这个http数据包的作用。继续分析：

注意到Server192.168.233.133主动向192.168.233.128的8888端口建立了tcp连接，然后192.168.233.128向192.168.233.133发送了大量数据。

这个过程说明server主机已经被控制。通过查找`Easy File Sharing Web Server`的相关漏洞，我们可以了解到这是一个存在于`Easy File Sharing Web Server`7.2版本的缓冲区溢出漏洞。而之前畸形的HTTP数据包就是漏洞的payload。

总结

到此，这个misc系列就告一段落了。

ALL1.pcapng.zip (0.743 MB) 下载附件
scan.pcapng.zip (0.056 MB) 下载附件
brust.pcapng.zip (0.017 MB) 下载附件

上一篇：DedeCMS前台鸡助Getshe... 下一篇：渗透技巧——利用图标文件获取连接文...

1. 7 条回复


老锥 2018-01-25 20:14:58

支持

0 回复Ta


han****@163.com 2018-01-26 13:58:17

不错，新手教程很合适

0 回复Ta

 M1n3 2018-05-06 19:45:13

@老锥 妈耶 老锥

0 回复Ta

 1815837370479554 2018-05-29 15:01:59

支持 支持

0 回复Ta

 四川民工返乡 2018-10-05 16:36:18

厉害了~~~~~~学习学习

0 回复Ta

 胖丫胖丫丶 2018-11-04 14:45:38

哇，学习学习。

0 回复Ta

 暮秋初九 2019-09-17 18:46:07

厉害了~学习学习

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板