i春秋 可恶的黑客

原创

H9_dawn 于 2020-04-11 16:20:00 发布 628 收藏 1

分类专栏： CTF 文章标签： web 安全

本文链接：https://blog.csdn.net/qq_43622442/article/details/105454269

CTF 专栏收录该内容

20 篇文章 2 订阅

订阅专栏

i春秋 可恶的黑客

过几天14号就是众测的考核了，听说有wireshark分析题，赶紧刷几道练练。

1.下载之后解压，用wireshark打开：

```
10.211.55.2      10.211.55.15     TCP       78 55535 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=780004401 TSecr=0 SACK_PERM=1
10.211.55.15     10.211.55.2      TCP       74 80 → 55535 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=1440879 TSecr=780004401 WS=64
10.211.55.2      10.211.55.15     TCP       66 55535 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=780004401 TSecr=1440879
10.211.55.2      10.211.55.15     HTTP     468 GET / HTTP/1.1
10.211.55.15     10.211.55.2      TCP       66 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=0 TSval=1440880 TSecr=780004401
10.211.55.15     10.211.55.2      TCP     1514 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=1448 TSval=1440880 TSecr=780004401 [TCP segment of a reassembled
10.211.55.15     10.211.55.2      HTTP     479 HTTP/1.1 200 OK  (text/html)
```

2.我真的很菜啊，难道要从这开头的三次握手一步一步往下看，这么多我要看到死= =想到题目是可恶的黑客，应该会有注册、登录、上传shell一些操作，我就过滤一下包：http.request.method==“POST”(还好学过

http.request.method=="POST"

No.	Time	Source	Destination	Protocol	Length	Info
123	7.651393	10.211.55.2	10.211.55.15	HTTP	674	POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)
129	7.666468	10.211.55.2	10.211.55.15	HTTP	796	POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)
134	9.690182	10.211.55.2	10.211.55.15	HTTP	442	POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)
162	52.468546	10.211.55.2	10.211.55.15	HTTP	506	POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)
168	52.471408	10.211.55.2	10.211.55.15	HTTP	796	POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)
173	59.273415	10.211.55.2	10.211.55.15	HTTP	442	POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)
185	89.581049	10.211.55.2	10.211.55.15	HTTP	486	POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)
191	89.583972	10.211.55.2	10.211.55.15	HTTP	796	POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)
196	91.816924	10.211.55.2	10.211.55.15	HTTP	442	POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)
208	134.513234	10.211.55.2	10.211.55.15	HTTP	490	POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)
214	134.516734	10.211.55.2	10.211.55.15	HTTP	796	POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)
219	137.115374	10.211.55.2	10.211.55.15	HTTP	442	POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)

> Frame 456: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits) on interface 0

3.清一色的1.php= =发现有个包不同：

456	440.456592	10.211.55.2	10.211.55.15	HTTP	212	POST /upload/example1.php HTTP/1.1 (text/plain)
480	473.149445	10.211.55.2	10.211.55.15	HTTP	796	POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)

4.追踪一下http流看干了些什么：

Wireshark · 追踪 HTTP 流 (tcp.stream eq 16) · 可恶的黑客.pcapng

```
GET / HTTP/1.1
Host: 10.211.55.15
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_5) AppleWebKit/603.2.4 (KHTML, like Gecko) Version/10.1.1 Safari/
603.2.4
```

```
Referer: http://10.211.55.15/xml/example1.php?xml=%3Ctest%3Ehacker%3C/test%3Eflag.txt
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate

HTTP/1.1 200 OK
Date: Wed, 09 Aug 2017 02:48:00 GMT
Server: Apache/2.2.16 (Debian)
X-Powered-By: PHP/5.3.3-7+squeeze15
X-XSS-Protection: 0
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1564
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>PentesterLab &raquo; Web for Pentester</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta name="description" content="Web For Pentester">
    <meta name="author" content="Louis Nyffenegger (louis@pentesterlab.com)">

    <!-- Le styles -->
    <link href="/css/bootstrap.css" rel="stylesheet">

    <style type="text/css">
      body {
        padding-top: 60px;
        padding-bottom: 40px;
```

分组 349。4 客户端 分组，4 服务器 分组，1 turn(s). 点击选择。

整个对话（36 kB） 显示和保存数据为 ASCII

查找： 查找下一个(N)

滤掉此流 打印 Save as… 返回 Close Help

5.大概也就是访问网站、访问了一张图片，然后访问了/upload/example1.php，然后上传了一个hnt.txt：

```
POST /upload/example1.php HTTP/1.1
Host: 10.211.55.15
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryBMPTIeB4An19V1ou
Origin: http://10.211.55.15
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_5) AppleWebKit/603.2.4 (KHTML, like Gecko) Version/10.1.1 Safari/
603.2.4
Referer: http://10.211.55.15/upload/example1.php
Content-Length: 384
Accept-Language: zh-cn

------WebKitFormBoundaryBMPTIeB4An19V1ou
Content-Disposition: form-data; name="image"; filename="hnt.txt"
Content-Type: text/plain

&#102;&#49;&#97;&#103;&#123;&#115;&#105;&#49;&#49;&#121;&#98;&#48;&#121;&#101;&#109;&#109;&#109;&#125;
------WebKitFormBoundaryBMPTIeB4An19V1ou
Content-Disposition: form-data; name="send"

Send file
------WebKitFormBoundaryBMPTIeB4An19V1ou--
HTTP/1.1 200 OK
Date: Wed, 09 Aug 2017 02:48:09 GMT
Server: Apache/2.2.16 (Debian)
X-Powered-By: PHP/5.3.3-7+squeeze15
```


6.发现有串html编码的字符，直接丢导航栏访问：

搜索 f1ag{si11yb0yemmm} 搜狗搜索

网页 新闻 微信 知乎 图片 视频 明医 英文 问问 学术 更多

这里要把1改成l