

BUUCTF Misc wireshark 1

原创

m0_55842055 于 2021-10-13 22:41:09 发布 51 收藏

文章标签: [wireshark](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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/m0_55842055/article/details/120753777

版权

wireshark 1

黑客通过wireshark抓到管理员登陆网站的一段流量包 (管理员的密码即是答案) 注意: 得到的 flag 请包上 flag{} 提交

CSDN @m0_55842055

题目很明显的提示就是用分析wireshark网络流量包的阅读

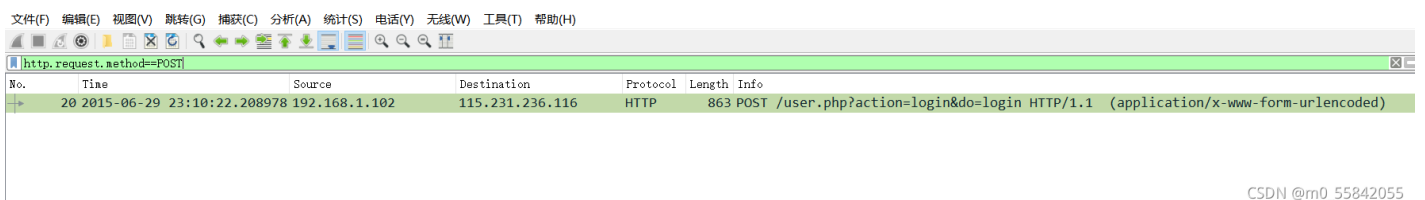
打开流量包,

第一个想法就是, 浏览一下从大部分中找小部分, 发现http比较特殊。

4	2015-06-29 23:10:19.530644	115.231.236.116	192.168.1.102	TCP	54	80 → 22429 [ACK]
5	2015-06-29 23:10:22.145604	192.168.1.102	115.239.211.92	TCP	66	22493 → 80 [SYN]
6	2015-06-29 23:10:22.147933	192.168.1.102	202.101.172.47	DNS	77	Standard query 0
7	2015-06-29 23:10:22.152404	202.101.172.47	192.168.1.102	DNS	293	Standard query r
8	2015-06-29 23:10:22.153446	115.239.211.92	192.168.1.102	TCP	66	80 → 22493 [SYN]
9	2015-06-29 23:10:22.153516	192.168.1.102	115.239.211.92	TCP	54	22493 → 80 [ACK]
10	2015-06-29 23:10:22.153953	192.168.1.102	115.239.211.92	HTTP	644	OPTIONS /v.gif?p
11	2015-06-29 23:10:22.162654	115.239.211.92	192.168.1.102	TCP	54	80 → 22493 [ACK]
12	2015-06-29 23:10:22.162766	115.239.211.92	192.168.1.102	HTTP	304	HTTP/1.1 200 OK
13	2015-06-29 23:10:22.195920	192.168.1.102	115.231.236.116	TCP	66	22494 → 80 [SYN]
14	2015-06-29 23:10:22.198675	192.168.1.102	202.101.172.47	DNS	72	Standard query 0
15	2015-06-29 23:10:22.201667	192.168.1.102	202.101.172.47	DNS	81	Standard query 0
16	2015-06-29 23:10:22.203882	202.101.172.47	192.168.1.102	DNS	297	Standard query r
17	2015-06-29 23:10:22.204326	202.101.172.47	192.168.1.102	DNS	284	Standard query r

第二个想法是: 从题目出发, 既然是上传登录信息, 就直接搜索 `http.request.method==post`

因为上传用户登录信息使用的一定是http里的post方法。



CSDN @m0_55842055

找到这个上传数据包后就可以在其中找登录的密码信息。

http.request.method==POST

No.	Time	Source	Destination	Protocol	Length	Info
20	2015-06-29 23:10:22.208978	192.168.1.102	115.231.236.116	HTTP	863	POST

- > Frame 20: 863 bytes on wire (6904 bits), 863 bytes captured (6904 bits)
- > Ethernet II, Src: LiteonTe_8d:1f:98 (74:de:2b:8d:1f:98), Dst: Tp-LinkT_a6:82:df (80:89:17:a6:82:df)
- > Internet Protocol Version 4, Src: 192.168.1.102, Dst: 115.231.236.116
- > Transmission Control Protocol, Src Port: 22494, Dst Port: 80, Seq: 1, Ack: 1, Len: 809
- > Hypertext Transfer Protocol
- ✓ HTML Form URL Encoded: application/x-www-form-urlencoded
 - > Form item: "email" = "flag"
 - > Form item: "password" = "ffb7567a1d4f4abdfdb54e022f8facd"
 - > Form item: "captcha" = "BYUG"

CSDN @m0_55842055

在HTML FROM URL RNCODED 中可以找到管理员用post上传的password