攻防世界 Misc高手进阶区 2分题 就在其中

原创

思源湖的鱼 于 2020-10-29 12:48:31 发布 712 收藏 1

分类专栏： ctf 文章标签： 网络安全 ctf 攻防世界 misc

本文链接：https://blog.csdn.net/weixin_44604541/article/details/109356633

前言

继续ctf的旅程

攻防世界Misc高手进阶区的2分题

本篇是就在其中的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

下下来一个流量包

wireshark打开

是tcp连接再ftp

估计是传文件

	Time	Source	Destination	Protocol	Length	Info
358	25.070226	192.168.1.108	192.168.1.106	FTP-D…	957	FTP Data: 891 bytes (
353	25.069525	192.168.1.106	192.168.1.108	TCP	74	54430 → 50068 [SYN] S
354	25.069622	192.168.1.108	192.168.1.106	TCP	74	50068 → 54430 [SYN, A
355	25.069742	192.168.1.106	192.168.1.108	TCP	66	54430 → 50068 [ACK] S
359	25.070346	192.168.1.106	192.168.1.108	TCP	66	54430 → 50068 [ACK] S
360	25.070398	192.168.1.108	192.168.1.106	TCP	66	50068 → 54430 [FIN, A

搜索关键词

找到key

```
03-12-16  12:20PM           142588562 IDA Pro 6.5 Setup.exe
08-09-16  11:15AM                 128 key.txt
08-10-16  11:29AM                 240 key.zip
08-09-16  11:12AM                 272 pub.key
08-09-16  11:11AM                 891 test.key
```

打开

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQD0UN0A+70iM0VCJ1ni0n/U1BRj0u8yMWH4Qi+xTbjHgbE7wOuk
OaO+2PyQXiqIzZnf5jCkJuVDYjALGcKrZM4OCQBBd85B/LTc36XZ7JVfX5kGy5tI
R3tquuPIVKNdAsHlSqh9S7YSS39RdnSa5rOUyGhrLzxwzzM9IO4e+QQ+CQIDAQAB
AoGADiaw5mGubtCxbkeBOVYf+V/fXnjVSf76QbrzsD1kOooUjfV6sKR2C5Pd7S7H
H+1owENBBgEKvoBtb/cqA2tvU9vQ4l5TMBJcHv6LEcb9WPpnMxPV2GNjO+DTPGPy
Xnu1UZlZjwx+NaF5rESoSSVS2ZaaIixBs4RWRXk+lHEbTFECQQD6Rp6jMweRgPHO
pR3mgIK83zL+kzqYM5isIPv3DIC5JQN2kXqK73IDQCFVlfXnr9lAAVRzLDsAXLqv
le/o6yQLAkEA+edY+GERlLuD1t2k9Js0Dc7EwnLcxoFUE60ivj8Gf9jzLskGHxsv
0IV6J5OHwPh54kAxAnqCjSqNRAWGNzr+uwJBALYEjDUm1LdGrxXZ0jAkgHC6Z0zs
aK3uwHdXGcinqCp+t9EQpq3KzQF+L4AeKxRQONEq5m9I2LQ/vGocwrmD4dcCQQDb
rTyOinWz8upAFPKOe2hUwvA/pkzgyosoCMhDyI9kD0gmVlvlODbd7Jem9o8dWM97
zcXHUf41LbSkmN6U6m1FAkEAqmZbr35bPfkeoiikwNl6OVQytg12TZjw2vIbvfub
f9Rvti8Lh/tbrmhZroiz8/l3aAZmugI1NBcbeZR0gz8ggg==
-----END RSA PRIVATE KEY-----
```


是个密钥
那应该还有个加密文件

尝试用foremost分离
得到key.txt

用openssl解密

```
openssl rsautl -decrypt -in key.txt -inkey rsa.key -out flag.txt
```

```
flag is {haPPy_Use_0penSsI}
```

得到flag

结语

知识点

- wireshark追踪流量
- foremost分离文件
- RSA加密